Bundesministerium
für Digitales und
Staatsmodernisierung

bundID

Schnittstellenbeschreibung

BundID (Nutzerkonto des Bundes)

Basisdienst ID und Postfach-Nachricht

12. Mai 2026

Überblick über das Dokument

Name des Dokuments	Schnittstellenbeschreibung BundID (Nutzerkonto des Bundes) Basisdienst ID und Postfach-Nachricht
Dokument-Version	1.0
Release-Version	11.1.1.0
Zweck des Dokuments	Beschreibung der Schnittstellen zum BundID Identity Provider sowie Beschreibung der Schnittstelle für den Nachrichtenversand an das Postfach in der BundID
Herausgebende Stelle	Bundesministerium für Digitales und Staatsmodernisierung, DS II 7
Stand	12.05.2026

Zusammenfassung

Dieses Dokument beschreibt die für Fachportale existierende SAML-Schnittstelle zum BundID Identity Provider (BundID IdP). Über diese Schnittstelle können Onlinedienste und Fachverfahren die Authentifizierung von Nutzerinnen und Nutzern über die BundID ansteuern. Im Kapitel 10 werden Beispiele für mögliche SAML-Anfragen an den BundID IdP sowie für die entsprechende Antworten aufgeführt.

Für das Postfach der BundID existiert die Komponente „Zentrales Bürgerpostfach“, welche über eine REST-Schnittstelle zur Anbindung verfügt. Die Dokumentation zur Postfach-Schnittstelle der BundID ist in einem gesonderten Dokument enthalten.

Versionshistorie

BundID – Basisdienst ID und Postfach-Nachricht (Zusammengeführtes Dokument)

Version	Beschreibung	Datum
0.94	Übernahme, Überarbeitung und Zusammenführung der AKDB-Dokumente	11.12.2019
0.95	Endabnahme	18.12.2019
0.97	Endabnahme	06.01.2020
0.98	Endabnahme	08.01.2020
0.99	Endabnahme	09.01.2020
1.0	Freigabe	16.01.2020
1.1	Zusatz UK Schnittstelle	11.03.2020
1.2	ITZBund Abnahme	03.04.2020
1.3	Korrekturen	15.05.2020
1.4	Korrekturen Verweise	18.05.2020
1.5	Korrekturen	05.06.2020
1.6	Korrekturen Verweise	22.06.2020
1.7	Korrektur 1 Schema Dateien	22.09.2020
1.8	Korrektur 2 Schema Dateien	24.09.2020
1.9	Kapitel Sondersituation Unternehmenskonto entfernt, Korrekturen Kap. 11, 12	02.10.2020
2.0	Erweiterungen in Kap. 5 und Kap. 6	10.11.2020
2.01	Korrekturen Kap 5. und Kap. 6	13.11.2020
2.02	Überarbeitung Kap 7.2 und Kap 8.4	11.02.2021
2.03	Korrekturen	16.02.2021
2.04	Entfernung „Künstlername“; Einarbeitung STORK-QAA-Level-3; Überarbeitung BSP-Quittung	11.03.2021

3.01	Ergänzung um Changes aus Release 3.1.0, redaktionelle Korrekturen, Entfernung Organisationskonto, Aufnahme Kap. 5.2 und 5.3, Anpassung Attribute in Kap. 6.1 und entspr. Hinweise, Entfernung Kap. 7, Kap. 8.3 ist obsolet, Aufnahme OZG-Hinweis in Kap. 11.2.5, Aufnahme Kap. 13 und 14	09.04.2021
3.02	Qualitätssicherung	20.04.2021
3.03	Korrektur technischer Begriff Postfach zu Postkorb	30.04.2021
3.2.0	Ergänzung um Changes Release 3.2.0.0, Kapitel 11.1.2, Kapitel 11.2.6 (Tabelle 9005), Kapitel 11.2.7	20.05.2021
3.2.1	Ergänzung um Changes Release 3.2.1.0, Kapitel 6.1, Kapitel 6.2.2, Kapitel 7.2, Kapitel 11.2.4	06.08.2021
3.2.1.1	Hotfix	09.09.2021
3.2.1.2	Hotfix und Aktualisierung 15.6.1 bspnachrichten-2.13.xsd	16.09.2021
4.0.0.0	Anpassung zu Release 4.0.0.0, Kapitel 6.2.6; Kapitel 8.3; Kapitel 9 eingefügt	16.11.2021
4.0.1.0	Kapitel 6 Hinweise zu Friendly Names, Kapitel 9.2 eingefügt	10.12.2021
4.0.1.0	Anpassung Logo und Bezeichnung BMI, Qualitätssicherung	21.12.2021
5.0.0.0	Überarbeitung Kapitel 8.3 und Kapitel 9 gesamt	04.04.2022
N/A	Qualitätssicherung	05.05.2022
5.0.2.0	Überarbeitung 6.1 und 9.1, Einarbeitung Kapitel 12.1.3	02.06.2022
N/A	Qualitätssicherung	07.07.2022
N/A	Ergänzung um Kapitel 10 SAML Beispiele, Überarbeitung Kapitel 11.2, Trennung SAML-Response Beispiele als Anhang 1 zur Schnittstellenbeschreibung	12.08.2022

N/A	Qualitätssicherung	18.08.2022
N/A	Redaktionelle Änderungen, Kapitel 9.4 eingefügt, Korrekturen Kap. 5.4 und 6.2.5	27.01.2023
N/A	Entfernung Kapitel 17.4, Qualitätssicherung	23.02.2023
N/A	Link unter Kapitel 6.1 Seite 20 aktualisiert	04.05.2023
N/A	Entfernung bPK, Version 1, Überarbeitung Kapitel 5.1, 6.1, 6.2.2, 7.2, 9.2, 9.4, 9.5	07.08.2023
N/A	Layout	17.10.2023
N/A	Überarbeitung Kapitel 9.2.1, 9.2.2, 9.4, Erweiterungen in Kapitel 6.1, 6.2.1, 9., 9.5, Aufnahme Kapitel 9.6 und 9.7	16.11.2023

Bitte beachten Sie, dass ab Mai 2024 eine neue Form der Dokumenten-Versionierung angewendet wird. Fortan gilt die Release-Version der Software als führend. Die Dokument-Version bezieht sich auf die für das Release geltende Schnittstellenbeschreibung und beginnt somit bei einem neuen Major-Release mit Version 1.0. Sollte es innerhalb eines Major-Releases zu Anpassungen in der Schnittstellenbeschreibung kommen, folgt Dokument-Version 2.0.

Release-Version	Dokument-Version	Beschreibung	Datum
9.0.0.0	1.0	Überarbeitung Kapitel 6, 6.1, 6.2.6, 7.1, 7.2 (Metadaten), 8.1, 8.2, 9, 9.3, 9.4, 13, 14, Erweiterung Kapitel 6.2.7, 6.2.8, Entfernung Kapitel 7.2 (Zusätzliche Metadaten) und 8.3	23.05.2024
9.0.0.0	2.0	Anpassung Kapitel 6.1 (Staatsangehörigkeit und Dokumententyp)	12.06.2024
9.1.0.0	1.0	Überarbeitung Kapitel 5.1, 5.5, 6.1, 9.4, Erweiterung Kapitel 2.1, 6.2.1, 6.2.2, 10.1, 10.2	26.09.2024
9.1.0.0	2.0	Anpassung Kapitel 6.2.1, 6.2.2	12.11.2024

10.1.0.0	1.0	Anpassung Kapitel 6.2.8, 9.5	17.04.2025
10.1.0.0	2.0	Korrekturen Kapitel 6.1	06.05.2025
10.2.0.0	1.0	Anpassung Kapitel 5, 5.3, 5.5, 6.2.10, 7.1, 9.2	16.05.2025
10.2.0.0	2.0	Korrekturen Kapitel 5 und 6	22.07.2025
11.0.0.0	1.0	Anpassungen Kapitel 1, 4, 5, 5.5, 6.1, 6.2.1, 6.2.2, 6.2.4, 6.2.9, 10.3, 10.4; Entfernen der Kapitel 11, 12, 13 und 14.	07.10.2025
11.1.0.0	1.0	Anpassung Kapitel 9.6	04.12.2025
11.1.1.0	1.0	Anpassung Kapitel 6.1	26.03.2026
11.1.1.0	1.1	Überarbeitung Kapitel 1, 2, 2.1, 3, 4, 4.2, 5.1, 5.2, 5.4, 5.5, 6.2.3, 6.2.7, 6.2.9, 7, 7.2, 8.1, 9, 9.2, 9.2.1, 9.2.2, 9.5	06.05.2026

Inhaltsverzeichnis

Zusammenfassung **1**

Versionshistorie **2**

1 Einleitung **9**

2 Das Bundesportal – eine offene Infrastruktur für Fachportale öffentlicher Verwaltungen **10**

2.1 Sichere Kodierung und Integration der BundID 10

3 Übersicht über die Funktionsweise der offenen Infrastruktur **12**

4 Unterstützte Anwendungsfälle **16**

4.1 Anwendungsfall 1 – direkte Tokennutzung 16

4.2 Anwendungsfall 2 – indirekte Tokennutzung 16

5 Unterstützte Authentisierungsverfahren und Anfragearten **18**

5.1 Auswahl bestimmter Authentisierungsverfahren 19

5.2 Besonderheiten bei der Nutzung von interoperablen Nutzerkonten 19

5.3 Besonderheiten bei der Nutzung der Methode "Temporär Login" 20

5.4 Kryptographische Vorgaben 20

5.5 Verwendung von Keycloak 21

6 Attribute im SAML-Token **22**

6.1 Personenbezogene Stammdaten 22

6.2 Technische Nutzdaten 26

6.2.1 bPK2 – bereichsspezifisches Personenkennzeichen 26

6.2.2 Vertrauensniveau 26

6.2.3 Version 27

6.2.4 AssertionProvedBy 28

6.2.5 Postkorb-Handle 28

6.2.6 Application ID (Antrags-ID) 29

6.2.7 Pseudonym 29
6.2.8 Vertrauensniveau der Attribute 30
6.2.9 SAML-Attribut für Zwei-Faktor-Authentifizierung 30
7 Betriebsvoraussetzungen 31
7.1 Infrastruktur 31
7.2 Metadaten 31
8 Entscheidungsunterstützung und Handreichungen 32
8.1 Architekturüberlegungen bei Auswahl eines SAML-Bindings 32
8.2 Zurückleiten in die Drittanwendung bei Abbruch durch Benutzer 32
9 Konfiguration der Anfrage 34
9.1 Einschränkung des Authentifizierungsverfahrens 34
9.2 Anforderung von Pflichtattributen 35
9.2.1 Technische Attribute vom Servicekonto und die Authentisierungsverfahren 37
9.2.2 Validieren von RequestedAttributes im SAML Request 38
9.2.3 Validieren von RequestedAttributes vor dem Absenden 38
9.3 Implementierungsanleitung BundID-Weiterleitung Modaldialog 38
9.3.1 Implementierungsbeispiel 42
9.4 Übergabe von UI-Information 44
9.5 Übergabe von UI-Informationen (seit Release 6) 44
9.6 Verwendete Fehlercodes am IDP bei unerwarteten SAML-Requests 46
9.7 Erweiterte Fehlermeldung im SAML-Response 47
10 Beispiele für SAML-Requests und SAML-Responses 48
10.1 Beispiele für SAML-Requests 48
10.2 Beispiele für SAML-Responses (entschlüsselter Bereich) 52
10.3 AKDB Extension Schema 55
10.4 UI Schema 57

11 Anhänge und Verzeichnisse 58

11.1 Abbildungen 58

11.2 Verweise auf externe Dokumente 58

11.3 Verwendete Abkürzungen 58

12 Quellen 59

1 Einleitung

Die BundID bildet über eine offene Infrastruktur mit den beteiligten Systemen den Portalverbund.

Die Bürgerinnen und Bürger legen eine individuelle BundID an und verwalten dort ihre persönlichen Daten und Zusatzinformationen. Die Befüllung der personenbezogenen Datenfelder für die BundID erfolgt entweder durch freiwillige Angaben (bei Registrierung ohne separates Zugangsmittel per Benutzername und Passwort) oder automatisiert durch das Auslesen der Daten des Zugangsmittels bei der Nutzung, z. B. mittels des Online-Ausweises.

Fachportale als Drittanwendungen im Portalverbund binden sich über definierte Standardprotokolle mittelbar an das Bundesportal an und profitieren im Sinne der Datensparsamkeit von der zentralisierten Verwaltung der personenbezogenen Nutzerdaten in der BundID.

In diesem Dokument wird die für Fachportale existierende Schnittstelle zum BundID Identity Provider beschrieben.

Hinweis Nutzerkonto BundID

Die URLs zur Nutzung der BundID Umgebungen (Integrations- und Produktionsumgebung) befinden sich im Anbindungsleitfaden der BundID, der im Downloadbereich des BundID Self Service Portals (BundID SSP) verfügbar ist.

2 Das Bundesportal – eine offene Infrastruktur für Fachportale öffentlicher Verwaltungen

Ausgewählte personenbezogene Daten aus dem Basisdienst „Nutzerkonto“ stehen im Rahmen einer offenen Infrastruktur auch einem weiteren Kreis an Drittanwendungen außerhalb des eigentlichen Bundesportals zur Verfügung (s. Kapitel 8 Entscheidungsunterstützung und Handreichungen).

Diese offene Infrastruktur basiert auf international anerkannten, quell-offenen Standardtechnologien [1] und sichert Drittanwendungen gegen unberechtigte Zugriffsversuche ab (d. h. ohne vorherige Autorisierung durch die ordnungsgemäßen Benutzer). Die von den Bürgerinnen und Bürgern dafür zu nutzenden Authentisierungsinformationen (u. a. Benutzername/Passwort, ePA-Pseudonym) sind identisch mit den im Bundesportal für die BundID hinterlegten Daten, sodass eine erneute Registrierung in den angebundenen Drittanwendungen entfällt.

Die an der BundID teilnehmenden Online-Leistungen werden als „Service-Provider“ bezeichnet und verbleiben damit sowohl in der rechtlichen als auch in der operativen Zuständigkeit derjenigen Körperschaft, in deren Namen die Dienstleistung den Bürgerinnen und Bürgern angeboten wird. Der Fortbestand eigener Web-Angebote erweist sich insbesondere in Fällen als sinnvoll, in denen ein hohes Maß an systemischer Komplexität gefordert oder das vorrangige Augenmerk auf den Schutz von langfristig getätigten, strategischen IT-Investitionen gelegt wird.

Die Auslagerung des Zugriffsschutzes von Drittanwendungen an Komponenten des Portalverbunds erfordert allerdings, abhängig vom Technologiestand des Service-Providers, einen nicht unerheblichen Eingriff in die bisherige Funktionsweise der Web-Anwendung. Aus technologischer Sicht lassen sich neu aufzubauende oder bestehende Applikationen, die bereits mit Standards wie OASIS SAML versehen sind, mit geringerem Aufwand in den Portalverbund integrieren als Anwendungen, die andersartige Zugriffskontrollmechanismen (wie z. B. Kerberos) nutzen.

2.1 Sichere Kodierung und Integration der BundID

Die BundID ist integraler Bestandteil eines umfassenden Systemverbunds und übernimmt dabei die Funktion eines Identity Providers (IdP). Gegenüber den Bürgerinnen und Bürgern stellt die BundID einen zentralen Vertrauensanker dar. Mit zunehmender Nutzung und Bekanntheit ist davon auszugehen, dass das System auch verstärkt als Angriffsziel in den Fokus rückt. Vor diesem Hintergrund ist es erforderlich, Sicherheitsrichtlinien, insbesondere zur sicheren Entwicklung, zu beachten und einzuhalten.

Neben den technischen Richtlinien des BSI, wie z. B. der BSI TR-03172-3, welche die Anforderungen zur sicheren Bereitstellung von Online-Verwaltungsleistungen beschreibt, wird auch auf die OWASP-Empfehlungen hingewiesen. Hier bieten beispielsweise die OWASP Secure Coding Practices, die OWASP Top Ten (häufigste Web-Sicherheitsrisiken) und der OWASP Developer Guide wertvolle Orientierung.

Unterstützung im Entwicklungsprozess kann darüber hinaus die Secure Developer Checklist bieten, die zur Definition sicherheitsrelevanter Kriterien, etwa in Scrum-Prozessen, genutzt werden kann. Für spezifische Anwendungsfälle, wie das SAML-basierte Single-Sign-On (SSO), ist das SAML Security Cheat Sheet eine hilfreiche Quelle.

Durch die Beachtung und Einhaltung dieser Sicherheitsvorgaben – von OWASP und BSI bis hin zu weiteren relevanten Standards – wird das Risiko von Sicherheitsvorfällen deutlich reduziert und die Integrität des Gesamtsystems bei der Integration der BundID nachhaltig abgesichert.

3 Übersicht über die Funktionsweise der offenen Infrastruktur

Im Detail stellt die Übersichtsgrafik den Authentisierungs- und Autorisierungsvorgang von Dienstnutzern im Zusammenspiel mit der offenen Infrastruktur und einer daran angebundenen Drittanwendung dar. Der abgebildete Ablauf in sieben Teilschritten folgt den international verbreiteten Standards der OASIS Group, wie sie auch im Kern der eCard-API des bundesdeutschen elektronischen Identifikationsmittel (ePA, eAT, EU-Karte) zum Einsatz kommen [2].

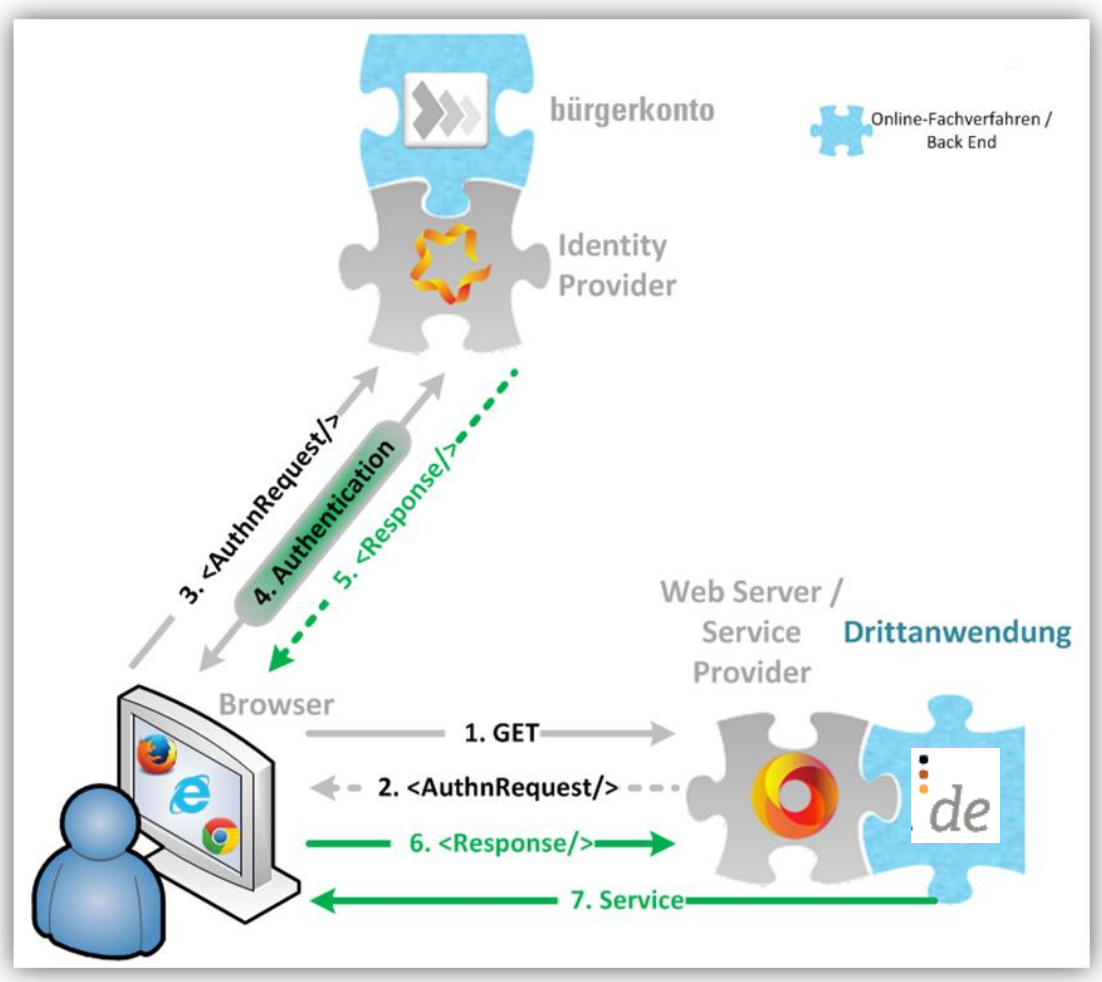

Abbildung 1: Zusammenspiel der Komponenten in der offenen Infrastruktur des Portalverbunds

Die einzelnen Teilschritte sind für die Dienstnutzer nur vereinzelt wahrnehmbar (wie aus den Screenshots ersichtlich) und erleichtern so die Handhabung des komplexen Authentisierungs- und Autorisierungsvorgangs:

Solange der Benutzer nicht authentisiert ist, kann lediglich auf die öffentlich zugänglichen Bereiche der Service-Provider-Applikation zugegriffen werden. Sobald eine zugriffsgeschützte Ressource im Web-

Angebot der Drittanwendung angefragt wird, wird der Zugriffsversuch auf Seiten des Service-Providers abgefangen (Schritt 1).

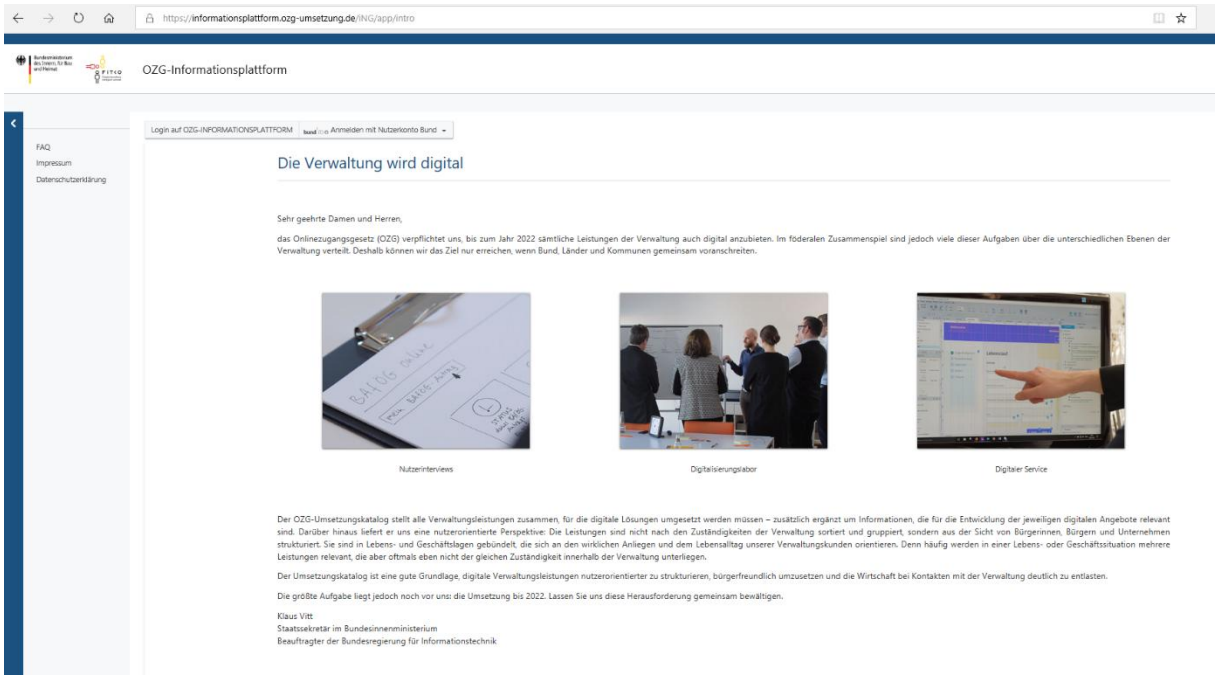

Abbildung 2: Öffentlich zugänglicher Bereich der Service-Provider-Applikation

Seitens des Fachportals wird daraufhin eine Authentisierungsanfrage an den BundID Identity-Provider als Authentisierungsinstanz gesendet, und der Benutzer wird dorthin umgeleitet. Derzeit geschieht dies in Form eines OASIS SAMLv2-konformen Authentication Requests via HTTP-REDIRECT oder HTTP-POST über den Browser des Benutzers (Schritt 2). Diese Anfrage wird nicht direkt an den Identity Provider versendet, sondern mittelbar über den Browser des Dienstanfragers weitergeleitet (Schritt 3).

Der Identity-Provider fordert den Dienstanfrager anschließend auf, sich ihm gegenüber durch ein vorkonfiguriertes Authentisierungsverfahren als bekannter Benutzer zu legitimieren. Dies kann beispielsweise durch den Abgleich von Benutzername und Passwort mit den im Bürgerkonto hinterlegten Daten oder durch die Nutzung der Online-Ausweisfunktion erfolgen. Erst nach erfolgreichem Abschluss der Authentisierung (Schritt 4) erfolgt am Identity Provider die Erstellung einer Antwortnachricht, die unter Hinzuziehung der in der BundID für die Person oder Organisation hinterlegten Daten erweitert wird. Ab diesem Zeitpunkt gilt der Dienstnutzer im rechtlichen Sinne als authentisierter Benutzer im Rahmen der Infrastruktur des Portalverbunds.

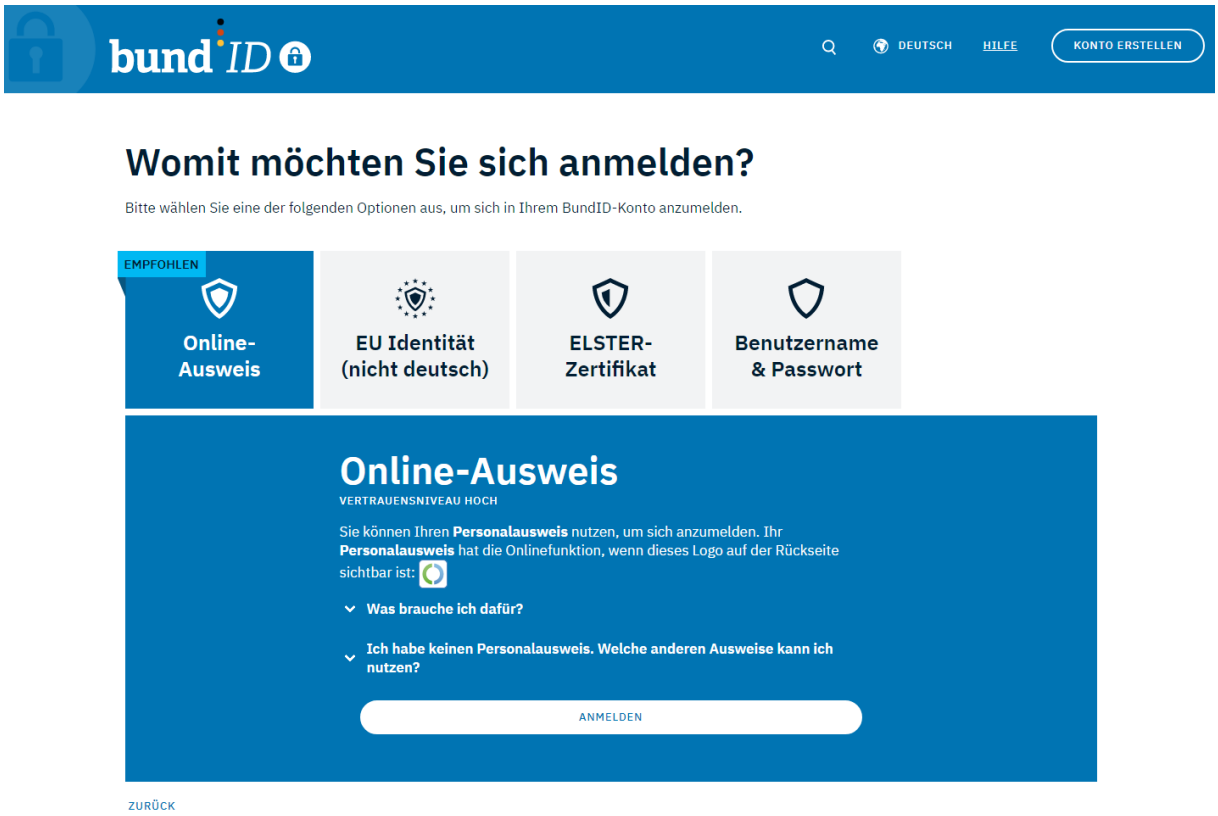

Abbildung 3: Authentisierung

Die erzeugte Antwortnachricht wird im Hintergrund als SAML-Response verschlüsselt und unter Einberechnung von Zertifikatsinformationen signiert (Schritt 5) an den Browser des potenziellen Dienstnutzers zurückgesendet. Von dort aus wird die SAML-Response an die Drittanwendung weitergeleitet. Die Verwendung BSI-konformer Verschlüsselungstechnologien [2] im vorherigen Schritt stellt sicher, dass der Dienstnutzer an dieser Stelle keine Möglichkeit zur Vortäuschung oder zur beabsichtigten Veränderung des Inhalts hat.

Der Service-Provider empfängt die SAML-Response (Schritt 6) und überprüft zunächst die Authentizität und Integrität der Nachricht. Anschließend wird überprüft, ob der Inhalt der vom Identity Provider stammenden Antwortnachricht den regelbasierten Erfordernissen der Drittanwendung genügt. Erst danach ist der authentisierte Dienstnutzer im rechtlichen Sinne autorisiert und zugriffsbefugt.

Der Service-Provider gewährt daraufhin den Zugriff auf die zunächst geschützte Ressource und führt die ursprüngliche Zugriffsanfrage aus. Die Antwort wird auf dem zugehörigen Anwendungsserver generiert und an den Browser des Dienstnutzers gesendet (Schritt 7).

Für den Zeitraum der weiteren Sitzung wird fortan die Auslieferung aller weiteren zugriffsgeschützten Ressourcen je nach Anfrage und applikationsspezifischem Verhalten erlaubt.

Darüber hinausgehende Zugriffsrestriktionen (z. B. nach RBAC) sind ausschließlich Bestandteil der Applikationslogik des Fachportals und liegen außerhalb des Funktionsumfangs der bereitgestellten Infrastruktur.

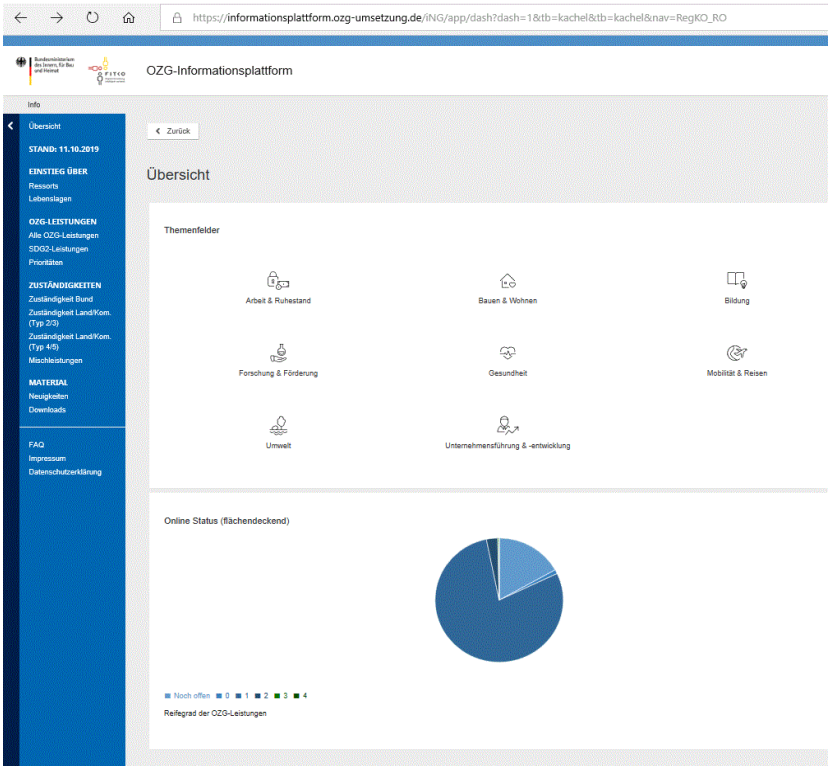

Abbildung 4: Geschützte Ressource – OZG-Informationsplattform

4 Unterstützte Anwendungsfälle

Die Online-Leistungen der (mittelbaren) Verwaltung binden sich an die BundID an und lagern die Nutzerauthentisierung an die Identity-Infrastruktur aus. Diese Service-Provider müssen als Endpunkt für [4] HTTP-REDIRECT oder HTTP-POST-Binding fungieren können.

Dies ist grundsätzlich über zwei Wege möglich:

1. Direkte Token-Generierung und -Nutzung innerhalb der Drittapplikation (z. B. über Open-Source-Bibliotheken)
2. Indirekte Token-Generierung und -Nutzung per Reverse-Proxy (z. B. über konfigurierbare Implementierungen verschiedener Hersteller)

4.1 Anwendungsfall 1 – direkte Tokennutzung

Die Drittanwendung kann direkt als Endpunkt für die Erzeugung von Authentication Requests und der Nutzung von SAML-Assertions fungieren. Dafür muss die Anwendung das bereits erwähnte OASIS SAMLv2 Web Browser Single-Sign-On-Profile implementieren.

Bei Wahl dieser ersten Betriebsvariante empfiehlt sich die Nutzung der Open-Source-Bibliothek OpenSAML oder ähnlicher Frameworks. Implementierungsbeispiele zur Nutzung finden sich z. B. im Entwickler-Paket von Governikus-Autent sowie in frei verfügbaren Quellen Dritter [4].

4.2 Anwendungsfall 2 – indirekte Tokennutzung

Erlaubt die Rechenzentrumsinfrastruktur den Betrieb von zusätzlichen Komponenten auf dem der Drittanwendung vorgelagerten Web-Server, bietet sich ergänzend die Nutzung von sogenannten Reverse-Proxy-Installationen an. Diese agieren als Endpunkt des SAML-Protokolls und verarbeiten die entsprechenden Requests und Responses für das Fachportal. Der Service-Provider besteht dann aus der eigentlichen Drittanwendung (dem webbasierten Fachverfahren) und dem vorgeschalteten Reverse Proxy als SAML-v2-Endpunkt.

Bei der Wahl dieser zweiten Betriebsvariante bietet sich die Nutzung von Reverse-Proxy-Produkten an, wie sie von Herstellern wie "ForgeRock" [5] oder "Shibboleth Consortium" [6] zur Verfügung stehen. Implementierungs- und Konfigurationsbeispiele zur Nutzung finden sich in den öffentlich zugänglichen

Produktdokumentationen der jeweiligen Hersteller und sind je nach Drittanwendung und Rechenzentrumsinfrastruktur einzelfallbezogen zu interpretieren.

Die im SAML-Token enthaltenen Attribute werden nach erfolgter Benutzeranmeldung in Abstimmung mit den Applikationsarchitekten als zusätzliche HTTP-Header-Attribute in die Online-Sitzung injiziert und stehen der Drittanwendung im weiteren Sitzungsverlauf zur weiteren Verarbeitung zur Verfügung.

5 Unterstützte Authentisierungsverfahren und Anfragearten

Die BundID verfügt über folgende Authentisierungsmethoden, die auch über ein zugehöriges Vertrauensniveau (s. Kapitel 6.2.2) eindeutig für Drittanwendungen erkennbar sind:

Bezeichnung	Ausgestaltung
Benutzername/Passwort (entspricht Nicht-Vertrauensniveau Basisregistrierung, STORK-QAA-Level-1)	• Ein Software-basiertes Verfahren • Die Registrierung erfolgt einzig durch Systemkomponenten
ELSTER-Zugang (entspricht Vertrauensniveau substanziell, STORK-QAA-Level-3)	• Ein Software-basiertes PKI-Verfahren • Die Registrierung und Nutzung erfolgt in Koordination mit den Systemkomponenten von ELSTER direkt
eID (Personalausweis, elektronischer Aufenthaltstitel, Unionsbürgerkarte) (entspricht Vertrauensniveau hoch, STORK-QAA-Level-4)	• Ein Hardware-basiertes PKI-Verfahren • Die Registrierung und Nutzung erfolgen in Koordination mit BSI-TR-zertifizierten eID-Servern
eIDAS (Vertrauensniveau ist unterschiedlich je nach Land)	• Ein Software-basiertes PKI-Verfahren • Authentifizierung mit eIDAS-notifizierten Identifikationsmittel
FINK (Föderiertes Identitätsmanagement Interoperabler Nutzerkonten in Deutschland) (Vertrauensniveau wird vom ausgewählten Nutzerkonto mitgegeben)	• Authentifizierung durch ein Nutzerkonto eines anderen Teilnehmers von FINK

5.1 Auswahl bestimmter Authentisierungsverfahren

Authentisierungsverfahren können nach Vertrauensniveau gruppiert und im Rahmen des SAML-AuthenticationRequests von einer Drittanwendung angefordert werden (sog. RequestedAuthnContext). Es wird der Comparison-Qualifier „minimum“ unterstützt. Die implizite Einschränkung von Authentisierungsmethoden über den Qualifier „exact“ ist obsolet und wird durch eine Extension im SAML-Request explizit gelöst.

Perspektivisch ist die Anbindung weiterer Authentifizierungsmittel geplant, die gemäß eIDAS-Verordnung notifiziert wurden. Diese können für die Authentifizierung auf den jeweiligen Vertrauensniveau-Stufen verwendet werden.

Für den Fall der indirekten Token-Nutzung (s. Kapitel 4.2 Anwendungsfall 2 – indirekte Tokennutzung) sind Erweiterungen über produktspezifische Konfigurationen vorzunehmen, so z. B. beim Reverse-Proxy des Herstellers „Shibboleth Consortium“ mittels Templates zum SessionInitiator [8].

Bei der Authentifizierung mit eIDAS liegen bislang keine Rückmeldungen von Service-Providern vor. Des Weiteren ist unklar, welche Art von ID bei einer temporären Anmeldung (ohne permanentes Nutzerkonto) übergeben wird und wie bzw. ob diese später wieder zugeordnet werden kann.

5.2 Besonderheiten bei der Nutzung von interoperablen Nutzerkonten

Im Rahmen des Föderierten Identitätsmanagements Interoperable Nutzerkonten in Deutschland (FINK), ist es möglich, dass die Authentifizierung durch ein Nutzerkonto eines anderen Teilnehmers von FINK durchgeführt wird. Hierbei wird der SAMLAuthenticationRequests an das ausgewählte Nutzerkonto weitergeleitet (siehe FINK Informationsplattform). Das ggfs. vorgegebene Vertrauensniveau wird dabei mitgegeben, sodass das empfangene Nutzerkonto entsprechend reagieren kann. Im Umkehrschluss reagiert das Nutzerkonto gleichermaßen.

Die Attributmenge kann je Nutzerkonto eines Teilnehmers variieren. Sofern ein PersonIdentifier mitgeliefert wird, werden diese Attribute aus Datenschutz-Gründen gefiltert und nicht verarbeitet.

Die Interoperabilität von Postfächern wird zu einem späteren Zeitpunkt bereitgestellt; insofern werden potenziell mitgelieferte Postfachreferenzen ebenfalls gefiltert und nicht verarbeitet.

Für weitergehende Informationen wird auf die Informationsplattform des FINK-Verbunds verwiesen:

https://informationsplattform.fink.services/

5.3 Besonderheiten bei der Nutzung der Methode "Temporär Login"

Gemäß des Onlinezugangsgesetzes (OZG) muss es Nutzenden möglich sein, das Nutzerkonto ohne Langzeitspeicherung von Daten verwenden und sich hierüber gegenüber Drittanwendungen authentifizieren zu können. Hierfür bietet das Nutzerkonto die Methode "Temporärer Login", welche am IdP als zusätzliche Methode angeboten wird. Für den temporären Login können alle elektronischen Identifikationsmittel verwendet werden, wie bspw. die Online-Ausweisfunktion. Zu beachten ist, dass bei dieser Methode auschließlich Daten ausgelesen und weitergegeben werden. Es erfolgt keine weitergehende Speicherung oder Verarbeitung der Daten. Dies hat zur Folge, dass die technischen Nutzdaten nur eingeschränkt bereitgestellt werden. Insbesondere entfallen bei dieser Methode das Postkorb-Handle und das bereichsspezifische Personenkennzeichen (bPK2).

Sofern eine Drittanwendung ohne diese Daten nicht nutzbar ist, muss das Error-Handling bei der Drittanwendung stattfinden und nicht im Nutzerkonto.

Ein Benutzername wird nicht als temporärer Login angeboten.

5.4 Kryptographische Vorgaben

Als Basis wird die technische Richtlinie TR-03116-4 „Kryptographische Vorgaben für Projekte der Bundesregierung“, Teil 4 Stand 2023, des BSI verwendet. Dabei wird insbesondere der Punkt Vorgaben für SAML/XML Security betrachtet. Jede Änderung am Nutzerkonto wird möglichst kompatibel umgesetzt; nicht jede Appliance unterstützt jedoch jede neue Vorgabe mit ausreichendem Vorlauf. Etwaige Probleme können daher erst in den Integrationstests vor der Produktivsetzung festgestellt werden. Die Vorgaben der TR-03116-4 am NK werden unterstützt; eine Abweichung ohne konkrete Begründung ist nicht vorgesehen. Die gleichen Vorgaben gelten auch für die Onlinedienste. Eine technische Überprüfung der Einhaltung dieser Vorgaben ist nicht vorgesehen. Diese Prüfung obliegt den einzelnen Onlineverfahren selbst.

Über die Metadaten können zwar eigene Algorithmen für EncryptionMethod, DigestMethod oder SigningMethod konfiguriert werden. Das Vorgehen ist jedoch nicht unterstützt, da es allgemeine Änderungen erschwert und in Self-Service-Portalen zur Verwaltung von Metadaten in der Regel keine Anwendung findet.

5.5 Verwendung von Keycloak

Wir möchten darauf hinweisen, dass seitens BundID keine Gewähr für die Funktionalität und Kompatibilität bei der Verwendung von Keycloak zwecks Anbindung der BundID übernommen wird.

Dennoch ist bekannt, dass einzelne Anbindungen eine Integration per Keycloak anstreben oder bereits einsetzen. Um dem gerecht zu werden, hat die BundID Keycloak-Behörden-Community Informationen zusammengestellt, die bei der Umsetzung dieses Vorhabens helfen können. Bitte beachten Sie, dass der Verweis seitens BundID auf die nachfolgenden Anleitungen ohne Gewähr auf Aktualität und Richtigkeit erfolgt. Wir übernehmen keine Haftung für Schäden, die aus der Verwendung dieser Informationen entstehen. Es wird empfohlen, zusätzlich die von der BundID offiziell unterstützen Anbindungsmechanismen zu nutzen, um eine reibungslose Funktionalität und Kompatibilität sicherzustellen.

Weitere Informationen zur Integration mit Keycloak stehen in folgender externer Dokumentation bereit: https://github.com/opdt/keycloak-extension-bundid.

Ergänzend dazu existiert mit dem sogenannten BundID-Simulator ein fachlicher Mock, der die Funktion der BundID auf Basis der BundID-Spezifikation nachbildet. Weitere Informationen stehen in folgender externer Dokumentation bereit: https://github.com/opdt/bundid-simulator.

6 Attribute im SAML-Token

Derzeit stellt die Identity Infrastruktur die nachfolgend aufgelisteten Attribute aus dem Bürgerkonto zur weiteren Nutzung in Fachportalen in Form von SAML-Assertions zur Verfügung. Die darin übermittelten Daten entsprechen immer dem zum Zeitpunkt der Token-Ausstellung aktuellen Datensatz im Bürgerkonto. Die Daten werden im UTF-8-Zeichensatz NFC-kodiert.

Hinweis:

Entsprechend des verwendeten Protokolls (Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0) (https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf) darf für das Mapping der Attribute nicht das XML Attribut "FriendlyName" verwendet werden, da diese Werte nicht stabil und zudem optional sind. Hierfür ist der SAML2 Formal Name (URN-notiert) zu verwenden, da es sich hierbei um eine gleichbleibende ID handelt.

6.1 Personenbezogene Stammdaten

Die unmittelbar personenbezogenen Stammdaten aus dem Bürgerkonto werden in LDAP-konformer Notation zur Verfügung gestellt. Die Konversion in LDAP-Notation orientiert sich an den IETF-Standards aus RFC 4519 [9] und RFC 4524 [10].

Bezeichnung	FriendlyName	SAML2 Formal Name (URN-notiert)	Hinweise
Vorname(n)	givenName	urn:oid:2.5.4.42	
Nachname	surname	urn:oid:2.5.4.4	
Emailadresse (optional)	mail	urn:oid:0.9.2342.19200300.100.1.3	
Strasse	postalAddress	urn:oid:2.5.4.16	
PLZ	postalCode	urn:oid:2.5.4.17	
Wohnort	localityName	urn:oid:2.5.4.7	
Land (Adresse)	country	urn:oid:1.2.40.0.10.2.1.1.225599	Als ISO 3166-1 alpha-2 gepflegt. Ein D von der eID oder eIDAS wird durch DE ersetzt.

Akad. Titel (optional)	personalTitle	urn:oid: 0.9.2342.19200300.100.1.40	
Anrede	gender	urn:oid:1.3.6.1.4.1.33592.1.3.5	Die Anrede wird als numerischer Wert nach ISO 5218:2004 codiert. 0 = unbekannt 1 = männlich 2 = weiblich 9 = keine Angabe / nicht zutreffend
Geburtsdatum	birthdate	urn:oid:1.2.40.0.10.2.1.1.55	Nach ISO 8601 im sog. extended Format in der Form JJJJ-MM-TT ohne weitere Zeitangabe
Geburtsort (optional)	placeOfBirth	urn:oid:1.3.6.1.5.5.7.9.2	
Geburtsname	birthName	urn:oid:1.2.40.0.10.2.1.1.225566	
Staatsangehörigkeit	nationality	urn:oid:1.2.40.0.10.2.1.1.225577	Als Ländercode wird nach ICAO für Deutschland der Wert „D“ verwendet. Ist kein Wert eingetragen, kann die Staatsangehörigkeit „D“ auch angenommen werden, wenn im Feld „Dokumententyp“ der Wert „ID“ vorhanden ist. Die Staatsangehörigkeit (Datengruppe 10, DG10) ist bei Personalausweisen (eID mit Dokumententyp „ID“) erst ab November 2019 mit dem Wert „D“ befüllt. Davor ist die DG10 bei Personalausweisen leer.
Dokumententyp	documentType	urn:oid:1.2.40.0.10.2.1.1.552255	Der Dokumententyp wird aktuell in folgenden Fällen übergeben: • Bei einer Anmeldung/ Gastanmeldung mit eID

			• Wenn es durch ein interoperables SK geliefert wird • Bei einer Anmeldung mit Elster, falls bei dem Zugang ein Dokumententyp hinterlegt wurde In anderen Fällen steht der Wert nicht zur Verfügung. Mögliche Werte werden in der Technische Richtlinie TR-03127 definiert (Verlinkung Stand Juli 2025).
De-Mail	DeMail	urn:oid:1.3.6.1.4.1.55605.7073787 5.1.1.1.7.1	
Telefonnummer	telephoneNumber	urn:oid:2.5.4.20	Darstellung ab 05/2021 (R3.2.0.0) als international gültige Telefonnummer; in der BundID seit 09/2021 produktiv
eIDAS-Issuing-Country	eIDAS-Issuing-Country	urn:oid:1.3.6.1.4.1.25484.494450.1 0.1	Basiert auf SendingMemberState (TR-03130 eID-Server), optional, ISO 3166-1 alpha-2
Wohnort-ID	communityId	urn:oid:1.3.6.1.4.1.25484.494450.5	Der Wert wird übergeben, wenn die Authentifizierung mit der eID durchgeführt wird. Falls der Wert beim Hinterlegen der eID im Nutzerkonto gespeichert wurde, wird die Wohnort-ID auch übermittelt, wenn andere Verfahren als die eID zur Authentifizierung verwendet werden. Der Wert wird bei der Authentifizierung mit der eID aktualisiert (analog zur Adresse). Das Feld wird in TR-03127 als Datengruppe DG18 beschrieben. Die Verfügbarkeit ist abhängig vom Betreiber des NKs.

Freitext Adresse	freeTextAddress	urn:oid:1.3.6.1.4.1.25484.494450.6	Unstrukturierte, ausländische Adresse. Mehrzeiliges Eingabefeld. Ersetzt die Eingabe Strasse, PLZ und Ort bei bestimmten Ländern. Die Verfügbarkeit ist abhängig vom Betreiber des NKs.

Bitte beachten:

Bei der Authentifizierung mit eIDAS-notifizierten Identifikationsmittel gilt der Mindestdatensatz nach eIDAS-VO, daher kann es zu einem reduzierten Datensatz kommen.

Siehe hierzu:

https://ec.europa.eu/digital-building-blocks/sites/spaces/DIGITAL/pages/467109280/eIDAS+eID+Profile

https://ec.europa.eu/digital-building-blocks/sites/spaces/EIDCOMMUNITY/pages/48762251/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS

6.2 Technische Nutzdaten

Darüber hinaus werden technische Nutzdaten zur erleichterten Datenpersistenz in Drittanwendungen, zum Kontext des Authentisierungsvorgangs und zu weiteren Schnittstellen (Postfach) bereitgestellt.

6.2.1 bPK2 – bereichsspezifisches Personenkennzeichen

Das bPK2 ist die Base64-encodierte, eigentliche ssPIN (sektor-spezifische Personen-Identifikations-Nummern), die aus der Bürgerkonto UUID abgeleitet ist. Das bPK2 (bereichsspezifisches Personenkennzeichen) dient in Anlehnung an die österreichische Bürgerkarten-Infrastruktur zur datenschutzfreundlichen, für die jeweilige Drittanwendung eindeutig geltenden Identifizierung eines Nutzers. Im sog. Exportformat wird diese als Base64-encodierte Zeichenkette generiert.

Bezeichnung	FriendlyName	SAML2 Formal Name (URN-notiert)
bPK2	bPK2	urn:oid:1.3.6.1.4.1.25484.494450.3

Eine typische bPK2 sieht wie folgt aus:

mcR9heGIqQj1dF0PqlhlETJcTJIrBo05DZtt8qyUiPE

Bei FINK wird der Identifier aus dem anderen SK übernommen und mit Prefixen versehen, damit keine Überschneidung mit existierenden bPK2s möglich ist.

Achtung: Sofern das bPK2 durch OD/FV genutzt wird, ist bei der Änderung der URL eines Onlinedienstes (OD) darauf zu achten, dass der Hostname der entityID nicht verändert wird. Eine Änderung des Hostnames der entityID verursacht abweichend generierte bPK2.

6.2.2 Vertrauensniveau

Informationen über die vom Benutzer gewählte Authentisierungsmethode zur Initialisierung der Sitzung werden mittelbar in Form einer akkumulierten Trustlevel-Angabe (d. h. zum Authentisierungsvorgang und zur Herkunft der Attribute aus der BundID) verfügbar gemacht.

Bezeichnung	FriendlyName	SAML2 Formal Name (URN-notiert)
Vertrauensniveau	EID-CITIZEN-QAA-LEVEL	urn:oid: 1.2.40.0.10.2.1.1.261.94

Aufgrund der strategischen Wichtigkeit des von der Europäischen Kommission geförderten Large-Scale-Pilot-Projekts STORK [11] und im Lichte der eIDAS-Verordnung [12] wurde bis zur Veröffentlichung entsprechender Technischer Richtlinien seitens des BSI der Trustlevel-Ansatz nach der STORK-Methodik gewählt [13]. Zum derzeitigen Zeitpunkt unterscheidet die Identity Infrastruktur folgende Trustlevel nach STORK, die zukünftig als Kategorien mehrere gleichrangige Authentisierungsmethoden beinhalten können:

Bezeichnung	Bedeutung für Drittanwendungen
STORK-QAA-Level-1	aktuelle Authentisierung mittels Benutzername/Passwort; registrierte Attributdaten ohne hoheitliche Prüfung (= selbstregistrierte BundID bzw. eIDAS-Äquivalent)
STORK-QAA-Level-3	aktuelle Authentisierung mittels ELSTER-Zertifikat; registrierte Attribute aus dem ELSTER Zertifikat (= ELSTER Zertifikat registrierte BundID bzw. eIDAS-Äquivalent)
STORK-QAA-Level-4	aktuelle Authentisierung mittels Online-Ausweisfunktion (ePA, eAT, EU-Karte); registrierte Attributdaten aus Ausweismittel (= eID-registrierte BundID bzw. eIDAS-Äquivalent)

6.2.3 Version

Das Attribut Version dient der Vorbereitung verbesserten Kommunikation von Änderungen. Damit können Service-Provider technisch feststellen, mit welcher fachlichen Version der Schnittstelle sie es zu tun haben und können besser darauf reagieren. Die initiale Version lautet 2020.2.1; als Konvention wird Calendar Versioning [14] verwendet.

Bezeichnung	FriendlyName	SAML2 Formal Name (URN-notiert)
Version	Version	urn:oid:1.3.6.1.4.1.25484.494450.1

6.2.4 AssertionProvedBy

Darüber wird die Quelle transportiert, die die Identität überprüft hat.

Bezeichnung	FriendlyName	SAML2 Formal Name (URN-notiert)
AssertionProvedBy	AssertionProvedBy	urn:oid:1.3.6.1.4.1.25484.494450.2

Liste der möglichen IDs:

- eIDAS
- eID
- ELSTER
- Benutzername
- FINK

6.2.5 Postkorb-Handle

Das Postkorb-Handle in seiner jetzigen Form kann als Eingabeparameter für die Zustellung von Postfachnachrichten genutzt werden. Um Nachrichten einem bestimmten Vertrauensniveau in der späteren Ansicht zuzuordnen, ist bei der Benutzung der eigenen Postfach-API zusätzlich noch das Vertrauensniveau mitzugeben.

Bezeichnung	FriendlyName	SAML2 Formal Name (URN-notiert)
Postkorb-Handle	legacyPostkorbHandle	urn:oid:2.5.4.18

Jeder BundID ist immer ein Postkorb-Handle zugeordnet, welches wiederum genutzt werden kann, um ein Postfach eindeutig zu referenzieren.

Der String ist eine UUID mit 36 Zeichen.

6.2.6 Application ID (Antrags-ID)

Ein Antrag gruppiert alle Nachrichten, Dokumente und Statusmeldungen im ZBP. Jede Statusmeldung wird über die Antrags-ID mit diesem Antrag verknüpft. Dies gilt auch für Nachrichten. Mehr und aktuelle Informationen dazu bietet der Statusmonitor. Eine Antrags-ID kann technisch seit Release 9 übergeben werden.

Bezeichnung	FriendlyName	SAML2 Formal Name (URN-notiert)
Application ID (Antrags-ID)	applicationId	urn:oid:1.3.6.1.4.1.25484.494450.4

Schema der FITKO zum Statusmonitor (Stand 20.12.2023): https://schema.fitko.de/statusmonitor/status-schema/0.9.0/status-update.schema.json

Der String ist eine UUID mit 36 Zeichen.

6.2.7 Pseudonym

Das Pseudonym transportiert die Pseudonyme anderer Systeme. Die Weitergabe des dienste- und kartenspezifischen Kennzeichens (DKK) aus der eID erfolgt, um einen Benutzer auch bei einer Gastanmeldung mit der eID über das Nutzerkonto nicht nur anhand des Mindestdatensatzes, sondern auch anhand einer ID wieder identifizieren zu können. Es besteht hierbei keine Garantie, dass das Pseudonym für eine Identität stabil bleibt (ein abweichendes Zugangsmittel liefert ein neues Pseudonym für dieselbe Identität).

Achtung: Ein Pseudonym ist nur in Verbindung mit dem Attribut AssertionProvedBy eindeutig (der Angabe der Art des Zugangsmittels). Das Nutzerkonto gibt die Daten aus der Quelle unverändert weiter; es kann nicht ausgeschlossen werden, dass bei unterschiedlichen Zugangsmittelarten dasselbe Pseudonym verwendet wird (z. B. bei eID, eIDAS, ELSTER).

Bezeichnung	FriendlyName	SAML2 Formal Name (URN-notiert)
Pseudonym	pseudonym	urn:oid:1.2.40.0.10.2.1.1.226699

6.2.8 Vertrauensniveau der Attribute

Die übermittelten Attribute können andere Vertrauensniveaus als die Authentisierung selbst aufweisen. Das Vertrauensniveau des SAML-Attributs wird über das Attribut akdb:TrustLevel übermittelt.

<saml2:Attribute FriendlyName="legacyPostkorbHandle" Name="urn:oid:2.5.4.18" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" akdb:TrustLevel="NORMAL" xmlns:akdb="https://www.akdb.de/request/2018/09">

Dabei sind folgende Werte analog zur TR 03160-1 definiert:

Vertrauensniveau	**Wert**	**alte Bezeichnung**
STORK-QAA-Level-1	Basisregistrierung	Untergeordnet*
STORK-QAA-Level-2	Niedrig	Normal*
STORK-QAA-Level-3	Substanziell	Substanziell
STORK-QAA-Level-4	Hoch	Hoch

Falls kein Vertrauensniveau ermittelt werden kann, wird das Attribut nicht übergeben, auch nicht als Basisregistrierung.

*alte Bezeichnung für das entsprechende Vertrauensniveau, vgl. TR 03107-1

6.2.9 SAML-Attribut für Zwei-Faktor-Authentifizierung

Das Attribut mfa mit OID urn:oid:1.3.6.1.4.1.25484.494450.7 kann an den Onlinedienst innerhalb der SAML Response zurückgegeben werden. Es gibt mittels der Werte “true” oder “false” an, ob die Authentifizierung des Nutzenden bei der BundID durch einen zweiten Faktor abgesichert war.

Bei einer Anmeldung mittels Zugangsmittel eID oder ELSTER ist dies immer der Fall; bei einer Anmeldung per Benutzername und Passwort ist dies optional möglich.

7 Betriebsvoraussetzungen

7.1 Infrastruktur

Das ITZBund als Betreiber der SAML-basierten Identity-Infrastruktur der BundID sichert die dauernde Erreichbarkeit folgender Komponenten zu:

- Identity-Provider für die unterstützten Authentisierungsmethoden

Drittanwendungen können in beliebiger Technologie und Nutzungsweise (vgl. Kapitel 4) entwickelt werden, unter der einzigen Maßgabe, dass sie das Web-Browser-SSO-Profil des OASIS SAML v2 Standards implementieren.

7.2 Metadaten

(Technische) Voraussetzung zur Teilnahme an der SAML-basierten Identity Infrastruktur ist:

- Bereitstellung der SAML-Metadaten seitens der Drittanwendung

Es ist darauf zu achten, dass

1. die einzureichenden Metadaten *kein Ablaufdatum* enthalten (validUntil-Attribut),
2. die Metadaten *kein ID-Attribut* enthalten,
3. die *entityID als URI in URL-Notation* mit https-Protokoll-Prefix ohne Portnummer anzugeben ist. Diese muss nicht(!) zwingend mit der tatsächlich genutzten URL-Domain übereinstimmen, ist aber in Zusammenhang mit dem Attribut bPK2 in dieser Notation anzugeben. Die Auswahl der entityID sollte nach Aufnahme in den Wirkbetrieb nicht(!) mehr verändert werden und sollte den Betreiber der Drittanwendung eindeutig identifizieren (nicht unspezifisch), wie folgendes Negativbeispiel zeigt „https://drittanwendung.com/serviceprovider“.

Erst nach Bereitstellung der SAML-Metadaten können dem Teilnehmer die Metadaten des Identity Providers (bzw. für Drittanwendungen innerhalb des ITZBund-RZ die URL zu den Federation-Metadaten) mitgeteilt werden.

Die Bekanntgabe der Metadaten des Identity Providers durch das ITZBund ist als technologische Schnittstelle für die Entwicklung einer Drittanwendung hinreichend.

Für die Integrationsumgebung wird auch die IP-Adresse des zu verbindenden Verfahrens benötigt; für die Produktionsumgebung ist dies nicht nötig.

8 Entscheidungsunterstützung und Handreichungen

8.1 Architekturüberlegungen bei Auswahl eines SAML-Bindings

Für die Anbindung einer Drittanwendung an die BundID werden derzeit die beiden Bindings HTTP-REDIRECT und HTTP-POST unterstützt. Beide Bindings haben nachfolgend erwähnte Vor- und Nachteile im Praxisbetrieb, die im Rahmen der Architekturüberlegungen seitens der Bereitsteller von Drittanwendungen abzuwägen sind.

Das HTTP-REDIRECT-Binding ermöglicht das Übersenden des SAMLRequests als HTTP-GET-Parameter in der Anfrage-URL an den Identity Provider. Es unterliegt folglich den individuell regulierbaren Längenbegrenzungen aller zwischen Drittanwendung und Identity Provider befindlichen aktiven und passiven Netzwerkkomponenten (z. B. Switches, Web-Application-Firewalls, Proxies, Web-Server, Personal Firewalls der Benutzer, etc.).

Bei Nutzung des HTTP-POST-Bindings wird der SAMLRequest innerhalb des HTTP-Body übermittelt, sodass aktive und passive Netzwerkkomponenten den Protokollablauf nicht in der gleichen Weise, wie oben beschrieben, negativ beeinflussen können. Andererseits ist die Nutzung der „Zurück"-Funktionalität bei einem gewollten Abbruch auf der Identity Provider-Seite browserabhängig beeinträchtigt. Die Folge kann eine Weiterleitungsschleife sein, die den Benutzer bei Abbruch des Loginvorgangs wiederholt auf den Identity Provider weiterleitet. Dieses Problem zeigt sich generell bei Nutzung des SAML-HTTP-POST-Bindings und ist kein Spezifikum der hier genutzten Produkte.

Tendenziell ist daher die Benutzung des HTTP-POST-Bindings zu bevorzugen.

8.2 Zurückleiten in die Drittanwendung bei Abbruch durch Benutzer

Aufgrund der Architektur der meisten Drittanwendungen bei Nutzung des HTTP-POST-Bindings ist besonderes Augenmerk auf die Usability des Zurück-Buttons zu legen. Für eine reibungslose Zurückleitung in die Drittanwendung ist ein geordnetes Session-Handling der Drittanwendung gefordert, um ein zyklisches erneutes Absenden eines SAML-Requests und dessen Interpretation als Replay-Attacke zu vermeiden.

Umgesetzt werden kann ein solches Vorgehen z. B. durch das Setzen und Prüfen eines zusätzlichen Cookies zum Zeitpunkt der Erstellung des SAML-Requests der Art:

```
if  found_AlreadySentSAMLRequestCookie():
     invalidate_AlreadySentSAMLRequestCookie()
     forwardTo(previousStatus)
else:
    set_AlreadySentSAMLRequestCookie()
    sendSAMLRequest(SAMLRequest)
```

9 Konfiguration der Anfrage

SAML unterstützt Extensions im SAML-Request. Dort können neben dem SAML-Standard Erweiterungen verwendet werden. Fachlich werden diese als AkdbExtension bezeichnet (im SAML-Request akdb:AuthenticationRequest). Beispiele für einen vollständigen SAML-Request sind unten aufgeführt.

Die Verwendung des AuthenticationRequests in Version 2 ist von den Betreibern des Nutzerkontos als verpflichtend konfiguriert. Ebenfalls ist die Übergabe des OrganizationDisplayName sowie der OnlineServiceID (entspricht der BMI-ID) verpflichtend.

Damit müssen im SAML-Request folgende Bedingungen verpflichtend erfüllt werden:

- Der Request muss signiert sein
- OrganizationDisplayName muss übergeben werden
- OnlineServiceID muss übergeben werden
- akdb:AuthenticationRequest in Version 2 muss verwendet werden
- akdb:RequestedAttributes müssen mindesten ein akdb:RequestedAttribute anfordern

Falls diese Bedingungen nicht erfüllt sind, antwortet der IdP direkt mit einer SAML-Response, da der Request nicht verarbeitet werden kann.

Über eine Extension ist es möglich, die Anfrage weiter anzupassen, als das dies mit Standard SAML-Elementen möglich wäre. Der SAML-Request muss signiert sein, damit die Extension ausgewertet wird.

Die Hülle der Anfrage sieht folgendermaßen aus:

```
<akdb:AuthenticationRequest xmlns:akdb="https://www.akdb.de/request/2018/09" Version="2">
</akdb:AuthenticationRequest>
```

Achtung: Version ist ein Pflichtfeld. Aktuell wird nur Version 2 unterstützt. Die nachfolgenden Abschnitte beschreiben jeweils ein Kindelement der Extension.

9.1 Einschränkung des Authentifizierungsverfahrens

Zusätzlich zu Kapitel 5.1, können die Authentifizierungsverfahren auch folgendermaßen eingeschränkt werden. Die Smart-eID kann nicht als dediziertes Verfahren angefordert werden, da sie fachlich mit der eID gleichgestellt werden soll.

Es werden die aufgelisteten Authentifizierungsverfahren herangezogen, die kein <akdb:Enabled> definiert haben oder deren Wert „true“ entspricht.

Version 2

```
<akdb:AuthnMethods>
    <akdb:Authega>
        <akdb:Enabled>true</akdb:Enabled>
    </akdb:Authega>
    <akdb:Benutzername>
        <akdb:Enabled>true</akdb:Enabled>
    </akdb:Benutzername>
    <akdb:eID>
        <akdb:Enabled>true</akdb:Enabled>
    </akdb:eID>
    <akdb:eIDAS>
        <akdb:Enabled>true</akdb:Enabled>
    </akdb:eIDAS>
    <akdb:Diia>
        <akdb:Enabled>true</akdb:Enabled>
    </akdb:Diia>
    <akdb:Elster>
        <akdb:Enabled>true</akdb:Enabled>
    </akdb:Elster>
    <akdb:FINK>
        <akdb:Enabled>true</akdb:Enabled>
    </akdb:FINK>
</akdb:AuthnMethods>
```

Die unterstützten Werte entsprechen denen aus Kapitel 6.3.5 (AssertionProvedBy). Die temporäre Anmeldung ist kein eigenständiges Verfahren, weswegen dieser nicht über diese Liste abgewählt werden kann.

9.2 Anforderung von Pflichtattributen

Im SAML Request können Pflichtattribute angefordert werden.

Die Änderung in Version 2 dient zur Gewährleistung der Datensparsamkeit, indem die Attribute spezifiziert werden müssen, deren Daten aus dem Nutzerkonto an den Aufrufer übertragen werden sollen. Eine implizite Rückgabe aller vorhandener Daten wird nicht mehr unterstützt; es werden ausschließlich die angefragten Daten übermittelt.

Achtung: Seit Version 2 ist <akdb:RequestedAttributes> **verpflichtend**, bei Nutzung des <akdb:AuthenticationRequest>. Es werden nur die Attribute zurückgeliefert, die aufgelistet sind. Fehlende <akdb:RequestedAttributes> oder leere <akdb:RequestedAttributes> führen dazu, dass die Extension im SAML-Request ignoriert wird. Mit RequiredAttribute können Attribute als verpflichtend gekennzeichnet werden. Dadurch wird garantiert, dass die Antwort (im Erfolgsfall) die verpflichtenden Attribute beinhaltet. Falls die erforderlichen Daten nicht vorliegen, wird eine SAML-Response als Fehler ohne Daten übertragen. RequiredAttribute ist per Default auf „false“ gesetzt.

Empfehlung zum Umgang mit Pflichtattributen

Es wird empfohlen, nur in begründeten Ausnahmen vom Standardfall abzuweichen und ein Attribut als verpflichtend (RequiredAttribute=true) anzugeben. Bei vielen Attributen besteht die Möglichkeit, dass diese im Einzelfall aus unterschiedlichen Gründen nicht vorhanden sind. Bei RequiredAttribute=true führt dies dazu, dass die SAML-Response einen Fehler enthält und der Prozess für den Nutzenden an der Stelle abbricht.

Insbesondere bei einem vorausgesetzten Nicht-Vertrauensniveau “Basisregistrierung” wird empfohlen, vollständig auf Pflichtattribute zu verzichten. Für den Antrag erforderliche Angaben können in diesem Fall im Antragsprozess des Onlinedienstes durch den Nutzenden ohne Verlust des Vertrauensniveaus angegeben werden. Auch bei einem höheren Vertrauensniveau, etwa “"substanziell”, wird ein zurückhaltender Einsatz von RequiredAttribute=true empfohlen. Die Identität des Nutzenden ist durch das VN entsprechend bestätigt; weitere Attribute sollten nur bei fachlicher Prüfung als verpflichtend markiert werden.

Hinweise zu nicht vorhandenen Attributen

Die Rückmeldung des Nutzerkontos an den Onlinedienst im Rahmen der Authentifizierung (die SAML-Response) basiert auch auf den Daten des Zugangsmittels, welches vom Nutzenden für den Authentifizierungsvorgang verwendet wird. So können Attribute vom Zugangsmittel nicht an das Nutzerkonto übermittelt worden sein (vgl. bspw. eIDAS) oder nicht auf dem Zugangsmittel vorhanden sein (bspw. Vorname oder Anschrift bei einer eID). Entsprechend können solche Attribute nicht an den Onlinedienst zurückgegeben werden. Das Nutzerkonto ermöglicht es dem Nutzer bei Registrierung mit Benutzername und Passwort auch, bestimmte Daten als “nicht zutreffend” zu deklarieren und somit nicht

zu befüllen, die i.d.R. vorhanden sein sollten. Diese sind: Vorname, Geburtsname, Geburtsort, Adresse/Anschrift. Der Nutzer hat im Nachhinein die Möglichkeit, diese Daten zu ergänzen. Um einer "Falschnutzung" dieses Features durch den Nutzenden entgegenzuwirken, kann der Onlinedienst ein Vertrauensniveau größer gleich "substanziell" anfordern, um zu gewährleisten, dass die Attribute von vertrauenswürdiger externer Stelle überprüft wurden.

Sollte entsprechend ein vom Onlinedienst angefragtes Attribut nicht vorhanden sein, wird dies nicht in der SAML-Response enthalten sein.

Version 2

```
<akdb:RequestedAttributes>
    <akdb:RequestedAttribute Name="urn:oid:2.5.4.18" RequiredAttribute="false" />
    <akdb:RequestedAttribute Name="urn:oid:1.2.40.0.10.2.1.1.149" RequiredAttrib-
ute="true" />
    <akdb:RequestedAttribute Name="urn:oid:1.3.6.1.4.1.25484.494450.3"/>
</akdb:RequestedAttributes>
```

Das XML Attribut Name muss SAML2 Formal Name (URN-notiert) sein.

9.2.1 Technische Attribute vom Servicekonto und die Authentisierungsverfahren

Es können nachfolgende Attribute angefordert werden:

- bPK2 (urn:oid:1.3.6.1.4.1.25484.494450.3)
- legacyPostkorbHandle (urn:oid:2.5.4.18)

Werden ein, mehrere oder alle Attribute angefordert, werden die Authentisierungsverfahren ausgeblendet, welche die geforderten Attribute nicht erfüllen.

Sofern eine Drittanwendung beispielhaft ein bPK2 zwingend erfordert, kann die Drittanwendung im SAML-Request mindestens eines der Attribute anfordern, um das Ausblenden der temporären Anmeldung zu erreichen.

Bitte beachten Sie, dass sich die Daten, die ein Verfahren liefert, über die Zeit ändern können. FINK wurde bei einer Anfrage nach bPK2 zuerst ausgeblendet; dieses Verhalten wurde über die Zeit angepasst, da mittlerweile auch über den Portalverbund Kennzeichen übertragen werden, jedoch noch kein passendes Attribut zur Unterstützung eines legacyPostkorbHandle vorhanden ist.

9.2.2 Validieren von RequestedAttributes im SAML Request

Requests mit einer leeren Liste von RequestedAttributes oder mit falsch formatierten Attribut-Namen führen zum Ausschluss des <akdb:AuthenticationRequest>. Der IdP verhält sich in diesen Fällen so, als wäre kein <akdb:AuthenticationRequest> übermittelt worden. Entsprechend gelten diese leeren Anfragen als Fehler, und der SAML-Request wird abgewiesen.

```
<akdb:RequestedAttributes>
</akdb:RequestedAttributes>
```

```
<akdb:RequestedAttributes>
    <akdb:RequestedAttribute Name="" />
</akdb:RequestedAttributes>
```

9.2.3 Validieren von RequestedAttributes vor dem Absenden

Falls die angeforderten Attribute vom Servicekonto nicht bereitgestellt werden können, wird im SAML Response mit SAML statuscode=urn:oasis:names:tc:SAML:2.0:status:RequestDenied geantwortet.

9.3 Implementierungsanleitung BundID-Weiterleitung Modaldialog

Für Onlinedienste besteht die Möglichkeit zur Einbindung eines Modal-Dialogs, der Nutzende vor dem Verlassen des Onlinedienst-Angebots darauf hinweist, dass die soeben ausgeführte Nutzenden-Aktion die Weiterleitung zu id.bund.id auslösen wird.

Dieser Modaldialog kannn wie folgt im Hinblick auf Layout, Design, Funktionalität eingebunden werden, damit die UX als optimal empfunden wird:

Pop-Up Dialog

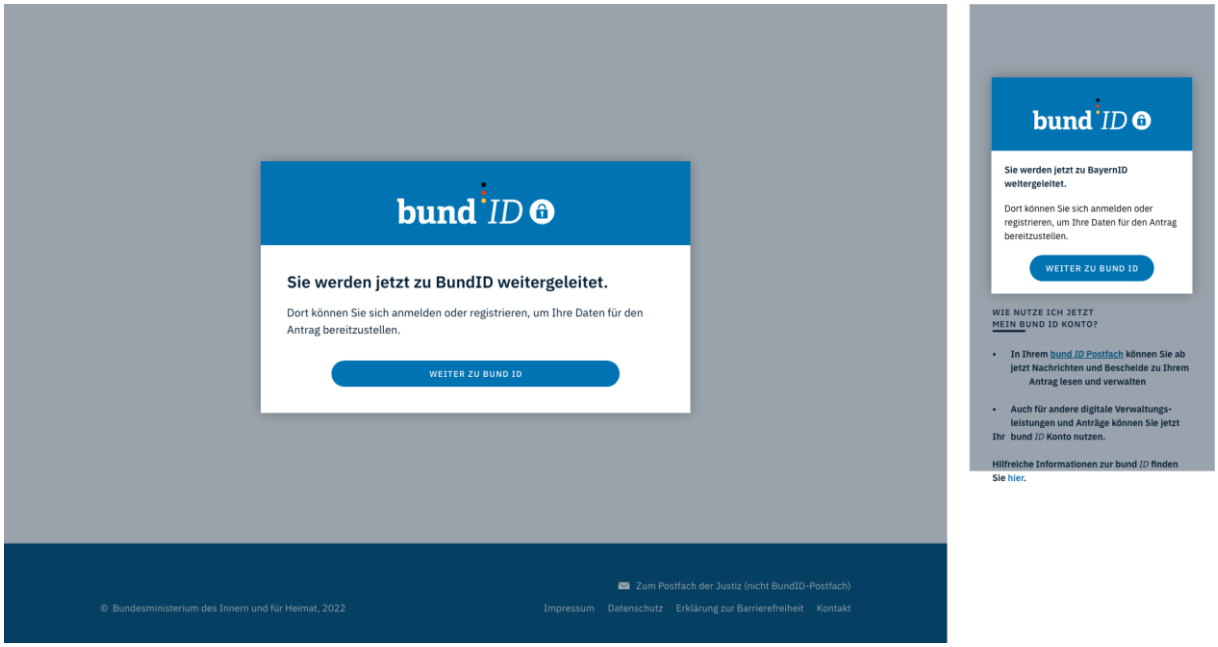

Abbildung 5: Pop-Up Dialog zur Weiterleitung an die BundID

Pop Up Mobile	Breite: 307 px / ca. 19 rem (Übernommen aus bekannten Maßen vom letzten Jahr) BITTE PRÜFEN Höhe Logo-Section (blau): **112px / 7rem** Höhe Gesamt: **flex**
Pop Up Desktop	Breite: **656px / 41rem** Höhe Logo-Section (blau): **128px / 8rem** Höhe Gesamt: **flex**
Farben	BundID-Blau: **#0074B3** Weiß: **#FFFFFF** Grau: **#666666** Schwarz: **#011D33**

Buttons Vorschau

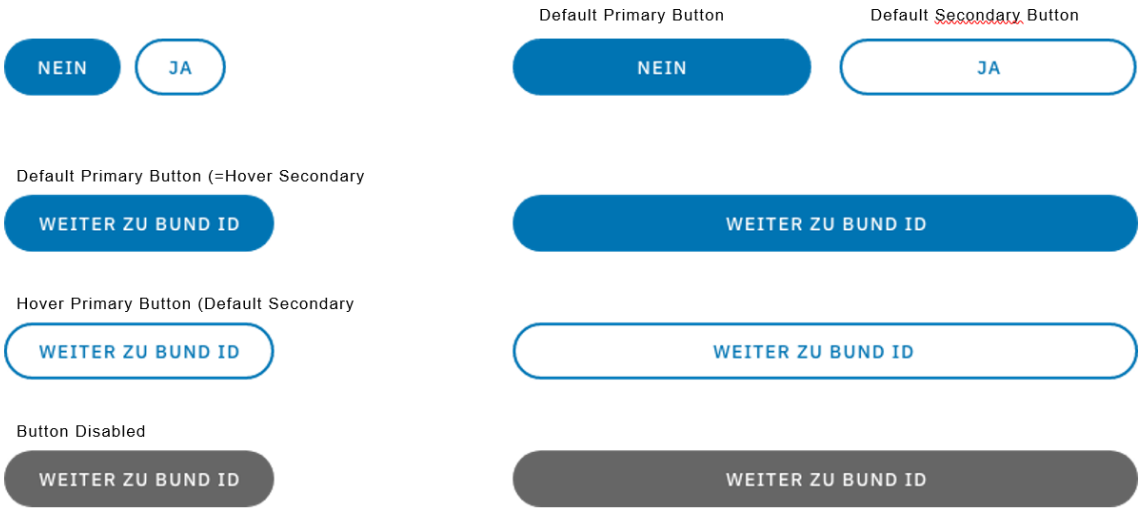

Abbildung 6: Buttons der BundID

Typografie Button (Desktop/ Tablet/ Mobile)	font: **IBM Plex Sans** font-hight: **14px** line-hight: **21px / 150 %** letter-spacing: **8 %**
Größe Button Mobile	Breite: 24 px / 1,5 rem Spacing + Labertext + 24 px / 1,5 rem Spacing) Spacing zwischen Buttons laut xd-File Mobile: 10 px Höhe (Standard-Höhe für Buttons BundID): **40px / 2,5rem**
Button Tablet/ Desktop	Breite wie bei IDP-Komponente: **500px / 32,25rem** Breite bei zwei Buttons je Button: **242px / 15,125rem** Abstand zwischen Buttons: **16px / 1rem** Höhe (Standard-Höhe für Buttons BundID): **40px / 2,5rem**

Desktop Details

Abbildung 7: BundID Desktop Details

Mobile Details

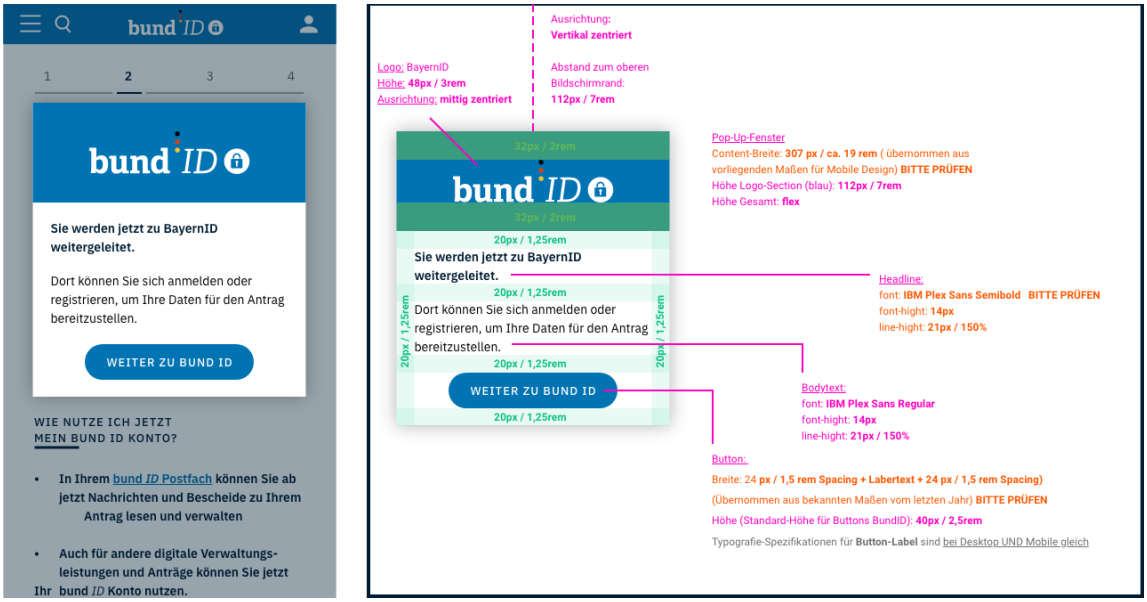

Abbildung 8: BundID Mobile Details

9.3.1 Implementierungsbeispiel

Das Beispiel verwendet zur Formatierung Tailwind CSS (https://tailwindcss.com/)

```
<div id="modal-container">

  <div data-modal="" data-test-id="db0f7modal-overlay" class="fixed inset-0 w-full h-screen last:bg-neutral last:bg-opacity-50 overflow-y-hidden flex items-center overscroll-none cursor-pointer" style="z-index: 1100;">

    <div class="max-h-screen max-w-fit overflow-auto mx-auto p-2">

      <div class="h-40 bg-primary flex justify-center items-center">

        <img class="text-skin-primary block justify-self-center h-24 scale-75 xxl:scale-100" src="/cms/assets/Logo_weiss-bunt.gJYOspMT.svg" alt="BundID" />

      </div>

      <div data-test-id="db0f7modal" class="bg-secondary flex shadow-lg cursor-auto" role="group" aria-live="polite" aria-label="modal" tabindex="0" aria-modal="true">

        <div class="flex flex-col m-2 overflow-auto relative" tabindex="0">

          <div id="modalContent" tabindex="-1" class="flex flex-col gap-5 justify-between mx-4 sm:mx-8 mb-12 mt-12" data-test-id="db0f7modal-content">

            <div class="max-w-[40rem]">

              <div class="flex flex-col text-styles">

                <h3 class="break-words">Sie werden jetzt zur BundID weitergeleitet.</h3>

                <p><p>Dort können Sie sich anmelden oder registrieren, um Ihre Daten für den Antrag bereitszustellen.</p></p>

              </div>

            </div>

             [BUTTON INTEGRIEREN siehe unten]

          <div><div><div></div></div></div>
```

Einen Button integrieren

```
<div class="grid gap-5 w-full mt-3 max-w-[28rem] mx-auto self-center grid-cols-1">

<button data-v-96f246fc="" class="transition duration-200 ease-out border-2 cursor-pointer min-h-[2.5rem] rounded-[1.25rem] text-spitzmarke bg-skin-primary text-skin-primary border-skin-primary hover:bg-skin-secondary hover:text-skin-secondary disabled:bg-skin-disabled disabled:text-skin-disabled disabled:border-skin-disabled" data-test-id="d0gQ0">

  <div data-v-96f246fc="" class="flex align-middle justify-between w-full relative items-

  center">

    <span data-v-96f246fc="" class="flex px-3"></span>
```

```
    <span data-v-96f246fc="" class="inline-block justify-self-center align-
    midle">WEITER</span>
    <span data-v-96f246fc="" class="flex px-3"></span>
  </div>
</button>
</div>
```

Zwei Buttons integrieren

```
<div class="grid gap-5 w-full mt-3 max-w-[28rem] mx-auto self-center grid-cols-[repeat(auto-fill,_minmax(12rem,_1fr))]">
   <button data-v-96f246fc="" class="transition duration-200 ease-out border-2 cursor-pointer min-h-[2.5rem] rounded-[1.25rem] text-spitzmarke bg-skin-primary text-skin-primary border-skin-primary hover:bg-skin-secondary hover:text-skin-secondary disabled:bg-skin-disabled disabled:text-skin-disabled disabled:border-skin-disabled" data-test-id="awwnM">
      <div data-v-96f246fc="" class="flex align-middle justify-between w-full relative items-center">
         <span data-v-96f246fc="" class="flex px-3"></span>
         <span data-v-96f246fc="" class="inline-block justify-self-center align-middle">ABBRECHEN</span>
         <span data-v-96f246fc="" class="flex px-3"></span>
      </div>
   </button>
   <button data-v-96f246fc="" class="transition duration-200 ease-out border-2 cursor-pointer min-h-[2.5rem] rounded-[1.25rem] text-spitzmarke bg-skin-primary text-skin-primary border-skin-primary hover:bg-skin-secondary hover:text-skin-secondary disabled:bg-skin-disabled disabled:text-skin-disabled disabled:border-skin-disabled" data-test-id="IRZBW">
      <div data-v-96f246fc="" class="flex align-middle justify-between w-full relative items-center">
         <span data-v-96f246fc="" class="flex px-3"></span>
         <span data-v-96f246fc="" class="inline-block justify-self-center align-middle">WEITER</span>
         <span data-v-96f246fc="" class="flex px-3"></span>
      </div>
   </button>
</div>
```

9.4 Übergabe von UI-Information

```
<akdb:DisplayInformation>
  <classic-ui:Version xmlns:classic-ui="https://www.akdb.de/request/2018/09/classic-ui/v1">
    <classic-ui:Purpose>
      <![CDATA[<h1>My HTML</h1>]]>
    </classic-ui:Purpose>
    <classic-ui:OrganizationDisplayName>
      <![CDATA[Meine Organisation>]]>
    </classic-ui:OrganizationDisplayName>
    <classic-ui:Lang>de</classic-ui:Lang>
    <classic-ui:BackURL>
      <![CDATA[https://example.com?a=1&b=2]]>
    </classic-ui:BackURL>
   <classic-ui:OnlineServiceId>
     <![CDATA[BMI-X0000]]>
   </classic-ui:OnlineServiceId>
  </classic-ui:Version>
</akdb:DisplayInformation>
```

9.5 Übergabe von UI-Informationen (seit Release 6)

Bei der Änderung des Einleitungstextes ist der Purpose auf allen Seiten am IdP sichtbar. Nur gewisse HTML Elemente (u. a. h1 p a b i) und Attribute (href auf a) sind erlaubt. Des Weiteren nur https-URLs für href.

Der Purpose bleibt in der Schnittstelle bestehen. Mit dem Redesign der BundID seit Release 6 wird jedoch der Purpose nicht mehr angezeigt.

OrganizationDisplayName wird vor der Übermittlung der Daten des Benutzers vom IdP an den Onlinedienst angezeigt. Bei Werten mit mehr als 50 Zeichen behalten wir uns vor, den Text im UI entsprechen zu kürzen. Aus Gründen der Abwärtskompatibilität wird im Übergangszeitraum bei fehlendem OrganizationDisplayName ein neutraler Wert angezeigt. Zuvor wurden die Daten aus den SAML-Metadaten aus Organization/OrganizationDisplayName verwendet, weswegen der technische Begriff hier wieder aufgenommen wurde. Fachlich wird der Wert auf https://id.bund.de auch im Kontext der Anmeldeinformationen für den Benutzer "Anmelden im Online-Verfahren "${OrganizationDisplayName}" verwendet (Stand 7. Juli 2023). Es besteht keine Anforderung, den Namen der Organisation zu übermitteln, die den SAML-Request stellt; vielmehr können fachlich hilfreiche Informationen übermittelt werden.

Lang kann verwendet werden, wenn im Onlinedienst bereits die gewünschte Sprache des Benutzers bekannt ist, damit dieser am SK nicht nochmals die Sprache wechseln muss. Valide Werte sind de, en. Der Wert ist optional und kann auch für Releases davor übergeben werden, hat dann aber keine Auswirkung. Der Default ist de.

BackURL wird für "zurück zum Onlinedienst" verwendet. Die Übergabe ist optional. Die URL wird nicht validiert, sollte aber https verwenden und keine Möglichkeit bieten, Zugriff auf Daten des Benutzers zu erlangen. Falls kein Wert übergeben wird, findet die Navigation zurück zum Onlinedienst über eine SAML-Response statt. Um Open-Redirects zu vermeiden, muss die URL vor der Übergabe im SAML-Requests validiert sein und darf nicht vom User verändert werden.

OnlineServiceId (seit Release 7) Im Schnittstellen-Request ist das Attribut mit dem Wert der ID zu verwenden, der in KOOPV durch das BMI bzw. BMDS vergeben wurde (die BMI-ID). Damit wird sichergestellt, dass trotz Verwendung geteilter Länder-Zertifikate eine eindeutige Erkennung des Onlinedienstes möglich ist. Die BMI-ID ist seit dem 30.06.2025 verpflichtend anzugeben.

```
<akdb:DisplayInformation>
  <classic-ui:Version xmlns:classic-ui="https://www.akdb.de/request/2018/09/classic-ui/v1">
    <classic-ui:Purpose>
      <![CDATA[<h1>My HTML</h1>]]>
    </classic-ui:Purpose>
    <classic-ui:OrganizationDisplayName>
      <![CDATA[Meine Organisation>]]>
    </classic-ui:OrganizationDisplayName>
    <classic-ui:Lang>de</classic-ui:Lang>
    <classic-ui:BackURL>
      <![CDATA[https://example.com?a=1&amp;b=2]]>
    </classic-ui:BackURL>
    <classic-ui:OnlineServiceId>
      <![CDATA[89479871264-DE]]>
    </classic-ui:OnlineServiceId>
  </classic-ui:Version>
</akdb:DisplayInformation>
```

9.6 Verwendete Fehlercodes am IDP bei unerwarteten SAML-Requests

Nicht alle Codes können zur gleichen Zeit auftreten und manche sind abhängig von der Konfiguration des jeweiligen Nutzerkontos. Der Code wird in der Regel in der Fehlerseite des NKs angezeigt und taucht in der URL als idp.code auf.

akdb-extension-missing
Anfrage mit fehlender AKDB-Extension.

akdb-extension-v1-deprecated
Anfrage mit veralteteter AKDB-Extension.

saml-request-not-signed
SAML-Request ist nicht signiert.

purpose-does-not-support-restricted-html
Purpose mit HTML, das nicht den Richtlinien entspricht.

missing-berca
Angefragtes Berechtigungszertifikat ist nicht hinterlegt.

requested-attributes-empty
Requested Attributes wurden nicht übergeben.

requested-attributes-missing-name
Requested Attributes ohne Name.

empty-authentication-methods
Leere Liste für Authentication Methods (keine Liste oder mind. ein Eintrag werden erwartet)

organization-display-name-missing
Name des Onlinedienstes fehlt.

online-service-id-missing
ID des Onlinedienstes fehlt.

9.7 Erweiterte Fehlermeldung im SAML-Response

Das Attribut EnableStatusDetail schaltet die erweiterte/detalierte Status-Meldung ein.

Das Setzen des Attributes

```
<akdb:AuthenticationRequest xmlns:akdb="https://www.akdb.de/request/2018/09" Version="2" Ena-
bleStatusDetail="true">
        ...
</akdb:AuthenticationRequest>
```

SAML-Response mit der detallierten Fehlermeldung

```
<saml2p:Response>
        ...
        <saml2p:Status>
                <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Requester">
                        <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:RequestDe-
                        nied"/>
                </saml2p:StatusCode>
                <saml2p:StatusMessage>security-msg</saml2p:StatusMessage>
                <saml2p:StatusDetail>
                        <akdb:StatusDetail xmlns:akdb="https://www.akdb.de/request/2018/09">
                                {
                                        "version": "1.0",
                                        "errors": [{
                                                "code": "IDP_REQUIRED_ATTRIBUTES_MISSING",
                                                "message":"Attribute
urn:oid:0.9.2342.19200300.100.1.20 is required but not available in Nutzerkonto. Attribute
urn:oid:0.9.2342.19200300.100.1.42 is required but not available in Nutzerkonto. Attribute
urn:oid:2.5.4.42 is required but not available in Nutzerkonto."
                                                }
                                        ]
                                }
                        </akdb:StatusDetail>
                </saml2p:StatusDetail>
        </saml2p:Status>
</saml2p:Response>
```

10 Beispiele für SAML-Requests und SAML-Responses

10.1 Beispiele für SAML-Requests

Beispiel für für SAML-Request V1

```
<saml2p:AuthnRequest
  xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
  AssertionConsumerServiceURL="https://samltool2-ewg.pre.buergerserviceportal.de/saml/SSO"
  Destination="https://id.bund.de/IdP/profile/SAML2/POST/SSO"
  ForceAuthn="true"
  ID="64e1f1b9-acf9-4076-b727-2833cd01200f"
  IsPassive="false"
  IssueInstant="2023-08-04T14:05:00.353Z"
  ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  Version="2.0">
  <saml2:Issuer
    xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
    https://samltool2-ewg.pre.buergerserviceportal.de
  </saml2:Issuer>
  <saml2p:Extensions>
    <akdb:AuthenticationRequest
       xmlns:akdb="https://www.akdb.de/request/2018/09"
       EnableStatusDetail="true"
       Version="2">
      <akdb:AuthnMethods>
        <akdb:Authega>
          <akdb:Enabled>
            true
          </akdb:Enabled>
        </akdb:Authega>
        <akdb:Benutzername>
          <akdb:Enabled>
            true
          </akdb:Enabled>
        </akdb:Benutzername>
        <akdb:eID>
          <akdb:Enabled>
            true
          </akdb:Enabled>
        </akdb:eID>
        <akdb:eIDAS>
          <akdb:Enabled>
            true
          </akdb:Enabled>
        </akdb:eIDAS>
        <akdb:Elster>
          <akdb:Enabled>
            true
          </akdb:Enabled>
        </akdb:Elster>
        <akdb:FINK>
          <akdb:Enabled>
            true
          </akdb:Enabled>
        </akdb:FINK>
      </akdb:AuthnMethods>
      <akdb:RequestedAttributes>
        <akdb:RequestedAttribute
          Name="urn:oid:1.3.6.1.4.1.33592.1.3.5"
          RequiredAttribute="false"
        />
        <akdb:RequestedAttribute
          Name="urn:oid:1.3.6.1.4.1.25484.494450.3"
          RequiredAttribute="true"
        />
        <akdb:RequestedAttribute
          Name="urn:oid:1.3.6.1.5.5.7.9.2"
          RequiredAttribute="false"
        />
        <akdb:RequestedAttribute
```

```
          Name="urn:oid:2.5.4.16"
          RequiredAttribute="false"
        />
        <akdb:RequestedAttribute
          Name="urn:oid:1.2.40.0.10.2.1.1.149"
          RequiredAttribute="false"
        />
        <akdb:RequestedAttribute
          Name="urn:oid:2.5.4.17"
          RequiredAttribute="false"
        />
        <akdb:RequestedAttribute
          Name="urn:oid:1.2.40.0.10.2.1.1.225599"
          RequiredAttribute="false"
        />
        <akdb:RequestedAttribute
          Name="urn:oid:1.2.40.0.10.2.1.1.225566"
          RequiredAttribute="false"
        />
        <akdb:RequestedAttribute
          Name="urn:oid:1.2.40.0.10.2.1.1.225577"
          RequiredAttribute="false"
        />
        <akdb:RequestedAttribute
          Name="urn:oid:2.5.4.18"
          RequiredAttribute="true"
        />
        <akdb:RequestedAttribute
          Name="urn:oid:0.9.2342.19200300.100.1.40"
          RequiredAttribute="false"
        />
        <akdb:RequestedAttribute
          Name="urn:oid:2.5.4.7"
          RequiredAttribute="false"
        />
        <akdb:RequestedAttribute
          Name="urn:oid:1.2.40.0.10.2.1.1.261.94"
          RequiredAttribute="false"
        />
        <akdb:RequestedAttribute
          Name="urn:oid:2.5.4.42"
          RequiredAttribute="false"
        />
        <akdb:RequestedAttribute
          Name="urn:oid:2.5.4.4"
          RequiredAttribute="false"
        />
        <akdb:RequestedAttribute
          Name="urn:oid:1.2.40.0.10.2.1.1.55"
          RequiredAttribute="false"
        />
        <akdb:RequestedAttribute
          Name="urn:oid:0.9.2342.19200300.100.1.3"
          RequiredAttribute="false"
        />
      </akdb:RequestedAttributes>
      <akdb:DisplayInformation>
        <classic-ui:Version
          xmlns:classic-ui="https://www.akdb.de/request/2018/09/classic-ui/v1">
          <classic-ui:Purpose>
            <![CDATA[Dieses Feld wird fachlich in der Schnittstelle akzeptiert, jedoch aktuell
nicht verwendet. Das ist aber zu Dokumentationszwecken weiterhin vorhanden. Von einer Verwen-
dung wird aber abgeraten.]]>
          </classic-ui:Purpose>
          <classic-ui:OrganizationDisplayName>
            <![CDATA[Der Name des Onlinedienstes kann hier gesetzt werden]]>
          </classic-ui:OrganizationDisplayName>
          <classic-ui:Lang>
            de oder en oder run oder uk (Abhängig der Sprachen des NKs)
          </classic-ui:Lang>
          <classic-ui:BackURL>
            <![CDATA[https://www.example.com/eine-url-zurueck?auch-mit=parametern]]>
          </classic-ui:BackURL>
          <classic-ui:OnlineServiceId>
```

```
            <![CDATA[Eine Onlinedienst-ID (fachliche Verwendung noch offen - also aktuell noch
nicht relevant)]]>
          </classic-ui:OnlineServiceId>
        </classic-ui:Version>
      </akdb:DisplayInformation>
    </akdb:AuthenticationRequest>
  </saml2p:Extensions>
  <saml2p:RequestedAuthnContext
    Comparison="minimum">
    <saml2:AuthnContextClassRef
      xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
      STORK-QAA-Level-1
    </saml2:AuthnContextClassRef>
  </saml2p:RequestedAuthnContext>
</saml2p:AuthnRequest>
```

Beispiel für SAML-Request V2

```
<saml2p:AuthnRequest
  xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
  AssertionConsumerServiceURL="https://samltool2-ewg.pre.buergerserviceportal.de/saml/SSO"
  Destination="https://id.bund.de/IdP/profile/SAML2/POST/SSO"
  ForceAuthn="true"
  ID="64e1f1b9-acf9-4076-b727-2833cd01200f"
  IsPassive="false"
  IssueInstant="2023-08-04T14:05:00.353Z"
  ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  Version="2.0">
  <saml2:Issuer
    xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
    https://samltool2-ewg.pre.buergerserviceportal.de
  </saml2:Issuer>
  <saml2p:Extensions>
    <akdb:AuthenticationRequest
       xmlns:akdb="https://www.akdb.de/request/2018/09"
       EnableStatusDetail="true"
       Version="2">
      <akdb:AuthnMethods>
        <akdb:Authega>
          <akdb:Enabled>
            true
          </akdb:Enabled>
        </akdb:Authega>
        <akdb:Benutzername>
          <akdb:Enabled>
            true
          </akdb:Enabled>
        </akdb:Benutzername>
        <akdb:Diia>
          <akdb:Enabled>
            true
          </akdb:Enabled>
        </akdb:Diia>
        <akdb:eID>
          <akdb:Enabled>
            true
          </akdb:Enabled>
        </akdb:eID>
        <akdb:eIDAS>
          <akdb:Enabled>
            true
          </akdb:Enabled>
        </akdb:eIDAS>
        <akdb:Elster>
          <akdb:Enabled>
            true
          </akdb:Enabled>
        </akdb:Elster>
        <akdb:FINK>
```

```
          <akdb:Enabled>
            true
          </akdb:Enabled>
        </akdb:FINK>
      </akdb:AuthnMethods>
      <akdb:RequestedAttributes>
        <akdb:RequestedAttribute
          Name="urn:oid:1.3.6.1.4.1.33592.1.3.5"
          RequiredAttribute="false"
        />
        <akdb:RequestedAttribute
          Name="urn:oid:1.3.6.1.4.1.25484.494450.3"
          RequiredAttribute="true"
        />
        <akdb:RequestedAttribute
          Name="urn:oid:1.3.6.1.5.5.7.9.2"
          RequiredAttribute="false"
        />
        <akdb:RequestedAttribute
          Name="urn:oid:2.5.4.16"
          RequiredAttribute="false"
        />
        <akdb:RequestedAttribute
          Name="urn:oid:1.2.40.0.10.2.1.1.149"
          RequiredAttribute="false"
        />
        <akdb:RequestedAttribute
          Name="urn:oid:2.5.4.17"
          RequiredAttribute="false"
        />
        <akdb:RequestedAttribute
          Name="urn:oid:1.2.40.0.10.2.1.1.225599"
          RequiredAttribute="false"
        />
        <akdb:RequestedAttribute
          Name="urn:oid:1.2.40.0.10.2.1.1.225566"
          RequiredAttribute="false"
        />
        <akdb:RequestedAttribute
          Name="urn:oid:1.2.40.0.10.2.1.1.225577"
          RequiredAttribute="false"
        />
        <akdb:RequestedAttribute
          Name="urn:oid:2.5.4.18"
          RequiredAttribute="true"
        />
        <akdb:RequestedAttribute
          Name="urn:oid:0.9.2342.19200300.100.1.40"
          RequiredAttribute="false"
        />
        <akdb:RequestedAttribute
          Name="urn:oid:2.5.4.7"
          RequiredAttribute="false"
        />
        <akdb:RequestedAttribute
          Name="urn:oid:1.2.40.0.10.2.1.1.261.94"
          RequiredAttribute="false"
        />
        <akdb:RequestedAttribute
          Name="urn:oid:2.5.4.42"
          RequiredAttribute="false"
        />
        <akdb:RequestedAttribute
          Name="urn:oid:2.5.4.4"
          RequiredAttribute="false"
        />
        <akdb:RequestedAttribute
          Name="urn:oid:1.2.40.0.10.2.1.1.55"
          RequiredAttribute="false"
        />
        <akdb:RequestedAttribute
          Name="urn:oid:0.9.2342.19200300.100.1.3"
          RequiredAttribute="false"
        />
```

```
      </akdb:RequestedAttributes>
      <akdb:DisplayInformation>
        <classic-ui:Version
          xmlns:classic-ui="https://www.akdb.de/request/2018/09/classic-ui/v1">
          <classic-ui:Purpose>
            <![CDATA[Dieses Feld wird fachlich in der Schnittstelle akzeptiert, jedoch aktuell
nicht verwendet. Das ist aber zu Dokumentationszwecken weiterhin vorhanden. Von einer Verwen-
dung wird aber abgeraten.]]>
          </classic-ui:Purpose>
          <classic-ui:OrganizationDisplayName>
            <![CDATA[Der Name des Onlinedienstes kann hier gesetzt werden]]>
          </classic-ui:OrganizationDisplayName>
          <classic-ui:Lang>
            de oder en oder run oder uk (Abhängig der Sprachen des NKs)
          </classic-ui:Lang>
          <classic-ui:BackURL>
            <![CDATA[https://www.example.com/eine-url-zurueck?auch-mit=parametern]]>
          </classic-ui:BackURL>
          <classic-ui:OnlineServiceId>
            <![CDATA[Eine Onlinedienst-ID (fachliche Verwendung noch offen - also aktuell noch
nicht relevant)]]>
          </classic-ui:OnlineServiceId>
        </classic-ui:Version>
      </akdb:DisplayInformation>
    </akdb:AuthenticationRequest>
  </saml2p:Extensions>
  <saml2p:RequestedAuthnContext
    Comparison="minimum">
    <saml2:AuthnContextClassRef
      xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
      STORK-QAA-Level-1
    </saml2:AuthnContextClassRef>
  </saml2p:RequestedAuthnContext>
</saml2p:AuthnRequest>
```

10.2 Beispiele für SAML-Responses (entschlüsselter Bereich)

```
<?xml version="1.0" encoding="UTF-8"?><saml2:Assertion xmlns:saml2="urn:oasis:na-
mes:tc:SAML:2.0:assertion" ID="_11a0a649e6bd232b84ca908e5f898ec4" IssueInstant="2023-08-
04T14:07:46.231Z" Version="2.0" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
    <saml2:Issuer>https://int.id.bund.de/IdP</saml2:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256"/>
            <ds:Reference URI="#_11a0a649e6bd232b84ca908e5f898ec4">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-sig-
nature"/>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                        <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-
c14n#" PrefixList="xsd"/>
                    </ds:Transform>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>JPRhAhjU5cJXh63HJuDaZ4rxXS+aYjlHL16YakDzuvE=</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>
        R27/7nb31O0ilgGiPDQCdJSEKr6NH8XErMwshrOl7x12mfaiOoDLxh9Q4LcCHZcsLV4lsiM-
pEdL/LO83elEXdU8eNU/fUsyxqD/proGr0CMxGxbqap4F1wv6vrpz1oA81/

FBUhWBmIHMR8IOT7R9EMmrM2aQ07XU8q601j9c4UKUv45AZ0KfTTgiO3nZ3awY/AHMg9lKVBmoGJpo3bNDWVynx1AR8VGQ
GsSLtu7hOAJfA2XQxSGbwtY0BT+9+OmAJjyR5r4WNlfz
        Qjr0SVYRZW20nOWLUj/G2ilt3ldyC2TOQ6zliUFtmUI00RlMFJlvJGQBPSr+jq7oL5HQgkQ+GQ==
        </ds:SignatureValue>
        <ds:KeyInfo>
            <ds:X509Data>
                <ds:X509Certificate>
                  MIIDGDCCAgCgAwIBAgIVAN5phAtPmCFBPamoDoX4vLS59JT4MA0GCSqGSIb3DQEBBQUAMBYxFDAS
```

```
                    BgNVBAMTC2lkcC5ha2RiLmRlMB4XDTEyMTAzMDA5NTY0MloXDTMyMTAzMDA5NTY0MlowFjEUMBIG
                    A1UEAxMLaWRwLmFrZGIuZGUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDD4sFNoPXy
                    JWRW+oI0JJwoXuQSqTi63VUlrRxYAObwjJdT7NLDJ0UyRwMSHvs7ggvEtT3nfvKKEpW01nQRa0Va
                    jrS2lEQTJKEOC28ikI3dlpbb6YIRcEaAEYIej99lIm4gNB4DS6XNUKD8yUvQr2Uijgpwp9Xn3EuC
                    5/LcxD464ubyyJqBZJfDn1+KFKGsA9YJomdppD5Xoce/MdlO6Eh5eEGSX2dyPRk02wVQtOjQImvM
                    Qhtv+JqLh3YxxRTqpay/NAhGJIRfvQk+iVuYMwlWvgWiUN3VsbYZwVj+3GiY+mz30q5CQt3ENi4I
                    OOonKqJKsX+kmuEfnC+/tiGImGqxAgMBAAGjXTBbMDoGA1UdEQQzMDGCC2lkcC5ha2RiLmRlhiJo
                    dHRwczovL2lkcC5ha2RiLmRlL2lkcC9zaGliYm9sZXRoMB0GA1UdDgQWBBQDriSLzK7LbBi6KZHK
                    Ij29z5kMHDANBgkqhkiG9w0BAQUFAAOCAQEAmc31v4QjVvHn5koO8ex/f+NyGOOgXXhWB7S7CcKz
                    X7ln89FVyzB02uEwUOYB48TgMLDKmMeBRbKyUumKhWh6Px42JWZjpQYJC2fj+w/axrnPSJsYq18v
                    uypuB3/EIlI6dX7g1519CfvAd9YEOXqIU1F4C+BIbgiomtgoQATGVxUKygHJbc5eI+Zfxv+KKFMy
                    QkU6AQBQ9UNTFn1UJCDqRTpFp1cju1BdCU5eX/FspCA33RmTeJtXGHkbKwakLyHb6Z3Z7hP9pUws
                    zwBZJkZW7O2G01U7iTXhLenuMM/Cg2sfJ0Fs8pOjRulzhDWrm28Cwrl2v73NQCc1m2Do2Fq7Og==
                  </ds:X509Certificate>
              </ds:X509Data>
          </ds:KeyInfo>
      </ds:Signature>
      <saml2:Subject>
          <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient" NameQualifier="https://int.id.bund.de/IdP"
            SPNameQualifier="https://samltool2-ewg.pre.buergerserviceportal.de">
            _ebb5259433f7e69608a59e32d0352d4f
          </saml2:NameID>
          <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
              <saml2:SubjectConfirmationData Address="93.199.14.87" InResponseTo="f83affde-7b9c-4987-93e2-907649f03647"
                NotOnOrAfter="2023-08-04T14:12:46.253Z" Recipient="https://samltool2-ewg.pre.buergerserviceportal.de/saml/SSO"/>
          </saml2:SubjectConfirmation>
      </saml2:Subject>
      <saml2:Conditions NotBefore="2023-08-04T14:07:46.231Z" NotOnOrAfter="2023-08-04T14:12:46.231Z">
          <saml2:AudienceRestriction>
              <saml2:Audience>https://samltool2-ewg.pre.buergerserviceportal.de</saml2:Audience>
          </saml2:AudienceRestriction>
      </saml2:Conditions>
      <saml2:AuthnStatement AuthnInstant="2023-08-04T14:07:43.661Z" SessionIndex="_8373c263f578eb77327fd61eafb4b1a6">
          <saml2:SubjectLocality Address="93.199.14.87"/>
          <saml2:AuthnContext>
              <saml2:AuthnContextClassRef>STORK-QAA-Level-4</saml2:AuthnContextClassRef>
          </saml2:AuthnContext>
      </saml2:AuthnStatement>
      <saml2:AttributeStatement>
          <saml2:Attribute FriendlyName="legacyPostkorbHandle" Name="urn:oid:2.5.4.18" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
            akdb:TrustLevel="NORMAL" xmlns:akdb="https://www.akdb.de/request/2018/09">
              <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">
              b980f78d-f5e0-45d9-8971-cc0e27f0beaf
              </saml2:AttributeValue>
          </saml2:Attribute>
          <saml2:Attribute FriendlyName="postalCode" Name="urn:oid:2.5.4.17" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
            akdb:TrustLevel="HOCH" xmlns:akdb="https://www.akdb.de/request/2018/09">
              <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">
              51147
              </saml2:AttributeValue>
          </saml2:Attribute>
          <saml2:Attribute FriendlyName="postalAddress" Name="urn:oid:2.5.4.16" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
            akdb:TrustLevel="HOCH" xmlns:akdb="https://www.akdb.de/request/2018/09">
              <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">
              HEIDESTRAßE 17
              </saml2:AttributeValue>
          </saml2:Attribute>
          <saml2:Attribute FriendlyName="givenName" Name="urn:oid:2.5.4.42" NameFor-mat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
            akdb:TrustLevel="HOCH" xmlns:akdb="https://www.akdb.de/request/2018/09">
              <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">
              ERIKA
```

```
            </saml2:AttributeValue>
        </saml2:Attribute>
        <saml2:Attribute FriendlyName="bPK2" Name="urn:oid:1.3.6.1.4.1.25484.494450.3" Name-
Format="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
          akdb:TrustLevel="NORMAL" xmlns:akdb="https://www.akdb.de/request/2018/09">
            <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">
            k2jBT0cykDVqiKWia1VMzqmntTu-EwGskIYlcCIGt_8
            </saml2:AttributeValue>
        </saml2:Attribute>
        <saml2:Attribute FriendlyName="placeOfBirth" Name="urn:oid:1.3.6.1.5.5.7.9.2" NameFor-
mat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
          akdb:TrustLevel="HOCH" xmlns:akdb="https://www.akdb.de/request/2018/09">
            <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">BERLIN</saml2:AttributeValue>
        </saml2:Attribute>
        <saml2:Attribute FriendlyName="country" Name="urn:oid:1.2.40.0.10.2.1.1.225599" Name-
Format="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
          akdb:TrustLevel="HOCH" xmlns:akdb="https://www.akdb.de/request/2018/09">
            <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">
              DE
            </saml2:AttributeValue>
        </saml2:Attribute>
        <saml2:Attribute FriendlyName="mail" Name="urn:oid:0.9.2342.19200300.100.1.3" NameFor-
mat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
          akdb:TrustLevel="NORMAL" xmlns:akdb="https://www.akdb.de/request/2018/09">
            <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">
            test.automat.nkb.aa@byom.de
            </saml2:AttributeValue>
        </saml2:Attribute>
        <saml2:Attribute FriendlyName="birthName" Name="urn:oid:1.2.40.0.10.2.1.1.225566"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
          akdb:TrustLevel="HOCH" xmlns:akdb="https://www.akdb.de/request/2018/09">
            <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">
            GABLER
            </saml2:AttributeValue>
        </saml2:Attribute>
        <saml2:Attribute FriendlyName="bPK" Name="urn:oid:1.2.40.0.10.2.1.1.149" NameFor-
mat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
          akdb:TrustLevel="NORMAL" xmlns:akdb="https://www.akdb.de/request/2018/09">
            <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">
            VlQ6OmRlLmFrZGIuYnBrLnNzb0BzYW1sdG9vbDItZXdnLnByZS5id-
WVyZ2Vyc2VydmljZXBvcnRhbC5kZTo6azJqQlQwY3lrRFZxaUtXaWExVk16cW1udFR
            1LUV3R3NrSVlsY0NJR3RfODo6MjAyMy0wOC0wNFQxNjowNzo0Mw==
            </saml2:AttributeValue>
        </saml2:Attribute>
        <saml2:Attribute FriendlyName="surname" Name="urn:oid:2.5.4.4" NameFor-mat="urn:oa-
sis:names:tc:SAML:2.0:attrname-format:uri"
          akdb:TrustLevel="HOCH" xmlns:akdb="https://www.akdb.de/request/2018/09">
            <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">
            MUSTERMANN
            </saml2:AttributeValue>
        </saml2:Attribute>
        <saml2:Attribute FriendlyName="localityName" Name="urn:oid:2.5.4.7" NameFor-
mat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
          akdb:TrustLevel="HOCH" xmlns:akdb="https://www.akdb.de/request/2018/09">
            <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">
            KÖLN
            </saml2:AttributeValue>
        </saml2:Attribute>
        <saml2:Attribute FriendlyName="gender" Name="urn:oid:1.3.6.1.4.1.33592.1.3.5" NameFor-
mat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
          akdb:TrustLevel="UNTERGEORDNET" xmlns:akdb="https://www.akdb.de/request/2018/09">
            <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">
            0
            </saml2:AttributeValue>
        </saml2:Attribute>
```

```
        <saml2:Attribute FriendlyName="EID-CITIZEN-QAA-LEVEL"
Name="urn:oid:1.2.40.0.10.2.1.1.261.94"
          NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" akdb:TrustLevel="NOR-
MAL" xmlns:akdb="https://www.akdb.de/request/2018/09">
            <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">
            STORK-QAA-Level-4
            </saml2:AttributeValue>
        </saml2:Attribute>
        <saml2:Attribute FriendlyName="birthdate" Name="urn:oid:1.2.40.0.10.2.1.1.55" NameFor-
mat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
          akdb:TrustLevel="HOCH" xmlns:akdb="https://www.akdb.de/request/2018/09">
            <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">
            1964-08-12
            </saml2:AttributeValue>
        </saml2:Attribute>
    </saml2:AttributeStatement>
</saml2:Assertion>
```

10.3 AKDB Extension Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
           elementFormDefault="qualified"
           targetNamespace="https://www.akdb.de/request/2018/09"
           xmlns:classic-ui="https://www.akdb.de/request/2018/09/classic-ui/v1"
           xmlns:akdb="https://www.akdb.de/request/2018/09">
    <xs:import namespace="https://www.akdb.de/request/2018/09/classic-ui/v1" schemaLoca-
tion="classic-ui.xsd"/>
    <xs:element name="AuthenticationRequest">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="akdb:AuthnMethods" minOccurs="0"/>
                <xs:element ref="akdb:RequestedAttributes"/>
                <xs:element ref="akdb:DisplayInformation"/>
            </xs:sequence>
            <xs:attribute name="EnableStatusDetail" use="optional" type="xs:boolean"/>
            <xs:attribute name="Version" use="optional" type="xs:integer" fixed="2"/>
        </xs:complexType>
    </xs:element>
    <xs:element name="AuthnMethods">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="akdb:Authega" minOccurs="0"/>
                <xs:element ref="akdb:Benutzername" minOccurs="0"/>
                <xs:element ref="akdb:Diia" minOccurs="0"/>
                <xs:element ref="akdb:eID" minOccurs="0"/>
                <xs:element ref="akdb:eIDAS" minOccurs="0"/>
                <xs:element ref="akdb:Elster" minOccurs="0"/>
                <xs:element ref="akdb:FINK" minOccurs="0"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:element name="Authega">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="akdb:Enabled"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:element name="Benutzername">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="akdb:Enabled"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:element name="Diia">
        <xs:complexType>
            <xs:sequence>
```

```
            <xs:element ref="akdb:Enabled"/>
        </xs:sequence>
    </xs:complexType>
</xs:element>
<xs:element name="eID">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="akdb:Berechtigungszertifikat"/>
            <xs:element ref="akdb:Enabled"/>
        </xs:sequence>
    </xs:complexType>
</xs:element>
<xs:simpleType name="state" final="restriction">
    <xs:restriction base="xs:string">
        <xs:enumeration value="BW"/>
        <xs:enumeration value="BY"/>
        <xs:enumeration value="BE"/>
        <xs:enumeration value="BB"/>
        <xs:enumeration value="HB"/>
        <xs:enumeration value="HH"/>
        <xs:enumeration value="HE"/>
        <xs:enumeration value="MV"/>
        <xs:enumeration value="NI"/>
        <xs:enumeration value="NW"/>
        <xs:enumeration value="RP"/>
        <xs:enumeration value="SL"/>
        <xs:enumeration value="SN"/>
        <xs:enumeration value="ST"/>
        <xs:enumeration value="SH"/>
        <xs:enumeration value="TH"/>
    </xs:restriction>
</xs:simpleType>
<xs:element name="Berechtigungszertifikat">
    <xs:complexType>
        <xs:attribute name="Bundesland" use="optional" type="akdb:state" />
    </xs:complexType>
</xs:element>
<xs:element name="eIDAS">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="akdb:Enabled"/>
        </xs:sequence>
    </xs:complexType>
</xs:element>
<xs:element name="Elster">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="akdb:Enabled"/>
        </xs:sequence>
    </xs:complexType>
</xs:element>
<xs:element name="FINK">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="akdb:Enabled"/>
        </xs:sequence>
    </xs:complexType>
</xs:element>
<xs:element name="RequestedAttributes">
    <xs:complexType>
        <xs:sequence>
            <xs:element maxOccurs="unbounded" ref="akdb:RequestedAttribute"/>
        </xs:sequence>
    </xs:complexType>
</xs:element>
<xs:element name="RequestedAttribute">
    <xs:complexType>
        <xs:attribute name="Name" use="required" type="xs:NMTOKEN"/>
        <xs:attribute name="RequiredAttribute" use="optional" type="xs:boolean"/>
    </xs:complexType>
</xs:element>
<xs:element name="DisplayInformation">
    <xs:complexType>
        <xs:sequence>
```

```
                <xs:element ref="classic-ui:Version"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:element name="Enabled" type="xs:boolean"/>
</xs:schema>
```

10.4 UI Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified" target-
Namespace="https://www.akdb.de/request/2018/09/classic-ui/v1" xmlns:classic-
ui="https://www.akdb.de/request/2018/09/classic-ui/v1" >
    <xs:element name="Version">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="classic-ui:Purpose" minOccurs="0"/>
                <xs:element ref="classic-ui:OrganizationDisplayName" minOccurs="1"/>
                <xs:element ref="classic-ui:Lang" minOccurs="0"/>
                <xs:element ref="classic-ui:BackURL" minOccurs="0"/>
                <xs:element ref="classic-ui:OnlineServiceId" minOccurs="0"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:element name="Purpose" type="xs:string"/>
    <xs:element name="OrganizationDisplayName" type="xs:string"/>
    <xs:element name="Lang" type="xs:NCName"/>
    <xs:element name="BackURL" type="xs:anyURI"/>
    <xs:element name="OnlineServiceId" type="xs:NCName"/>
</xs:schema>
```

11 Anhänge und Verzeichnisse

11.1 Abbildungen

Abbildung 1: Zusammenspiel der Komponenten in der offenen Infrastruktur des Portalverbunds 12

Abbildung 2: Öffentlich zugänglicher Bereich der Service-Provider-Applikation 13

Abbildung 3: Authentisierung 14

Abbildung 4: Geschützte Ressource – OZG-Informationsplattform 15

Abbildung 5: Pop-Up Dialog zur Weiterleitung an die BundID 39

Abbildung 6: Buttons der BundID 40

Abbildung 7: BundID Desktop Details 41

Abbildung 8: BundID Mobile Details 41

11.2 Verweise auf externe Dokumente

- Portalverbundvereinbarung
- Beitrittserklärung zum Portalverbund im Testbetrieb
- Beitrittserklärung zum Portalverbund im Wirkbetrieb
- Handreichung zum Nachweis der Beweiswerterhaltung bei Online Ausweis Funktion-Nutzung

11.3 Verwendete Abkürzungen

Kürzel	Ausführliche Benennung
SAML	Security Assertion Markup Language von OASIS
OASIS	Organization for the Advancement of Structured Information Standards
IdP	Identity Provider, die Authentisierungsinstanz
SP	Service-Provider, die Drittanwendung (ggf. inkl. Reverse Proxy)
SSO	Single Sign On
TLS	Transport Layer Security

12 Quellen

[1] OASIS SAML: http://saml.xml.org/saml-specifications

[2] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_1_ 2_Version_1_0.pdf?__blob=publicationFile

[3] http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

[4] http://www.capcourse.com/Library/OpenSAML/index.html

[5] http://forgerock.com/products/open-identity-stack/openig/

[6] https://shibboleth.atlassian.net/wiki/spaces/SP3/overview

[7] Beispiel am Ende der Herstellerdokumentation: https://wiki.shibboleth.net/confluence/display/SP3/SAML2+SessionInitiator

[8] https://tools.ietf.org/html/rfc4519

[9] https://tools.ietf.org/html/rfc4524

[10] https://tools.ietf.org/html/draft-gryphon-ldap-schema-vcard4-00#section-3.5

[11] https://ec.europa.eu/digital-agenda/en/trust-services-and-eid

[12] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

[13] https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=6:d32-qaa-status-report&Itemid=175) [Abrufdatum 14.06.2018]

[14] https://calver.org

[15] https://tools.ietf.org/html/rfc4519#section-2.25

[16] http://docs.oracle.com/cd/E19462-01/819-4670/gbanp/index.html

ozg-umsetzung.de